REPORT DOCUMENTATION PAGE

1. AGENCY USE ONLY (Leave Blank)	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	September 1994	Master's Thesis

4. TITLE AND SUBTITLE
AUTOMATIC IDENTIFICATION TECHNOLOGY (AIT):
THE DEVELOPMENT OF FUNCTIONAL CAPABILITY AND
CARD APPLICATION MATRICES (U)

5. FUNDING NUMBERS

6. AUTHOR(S)
Bower, Leslie Anne, LT, USNR

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Naval Postgraduate School
Monterey, CA 93943-5000

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/ MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSORING/ MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES
The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the United States Government.

12a. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for public release; distribution is unlimited.

12b. DISTRIBUTION CODE
A

13. ABSTRACT *(Maximum 200 words)*

Automatic identification technology (AIT), also known as automated data collection (ADC) technology, has been in use in various industry and government applications. The present AIT resources are magnetic ink character recognition, optical character recognition, bar code, magnetic stripe, radio frequency, optical laser memory, integrated circuit (IC), biometric and voice data collection, and machine vision. Smart card, super smart card, and magnetic memory card technology (e.g., PCMCIA) are integrated circuit technology. Personnel selecting, acquiring, implementing and using these technologies should possess a knowledge of the capabilities and applications of the AIT resources to obtain the best AIT system to meet their mission requirements.

In order to facilitate an understanding of the AIT resources and their applications, two matrices were developed. An AIT Functional Capability Matrix was developed to identify and assess the capabilities of the AIT resources. An AIT Card Application Matrix was developed to identify the automation of various applications with these technologies.

The matrices can assist system designers, system integrators, information systems management personnel, users, and consumers of AIT resources understand the functional capabilities and the applications of these technologies in a concise format. The matrices can be used for selection and acquisition of AIT systems and to track and address migration of the AIT systems throughout their life cycles.

14. SUBJECT TERMS
Automatic Identification Technology (AIT), Automatic Data Collection (ADC) Technology, Microcircuit Technology in Logistics Applications (MITLA)

15. NUMBER OF PAGES
207

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	Unclassified	Unclassified	UL

AUTOMATIC IDENTIFICATION TECHNOLOGY (AIT): THE DEVELOPMENT OF FUNCTIONAL CAPABILITY AND CARD APPLICATION MATRICES

by

Leslie A. Bower
Lieutenant, United States Naval Reserve
B.S., The Pennsylvania State University, 1982

Submitted in partial fulfillment of the
requirements for the degree of

**MASTER OF SCIENCE
INFORMATION TECHNOLOGY MANAGEMENT**

from the

NAVAL POSTGRADUATE SCHOOL
September 1994

ABSTRACT

Automatic identification technology (AIT), also known as automated data collection (ADC) technology, has been in use in various industry and government applications. The present AIT resources are magnetic ink character recognition, optical character recognition, bar code, magnetic stripe, radio frequency, optical laser memory, integrated circuit (IC), biometric and voice data collection, and machine vision. Smart card, super smart card, and magnetic memory card technology (e.g., PCMCIA) are integrated circuit technology. Personnel selecting, acquiring, implementing and using these technologies should possess a knowledge of the capabilities and applications of the AIT resources to obtain the best AIT system to meet their mission requirements.

In order to facilitate an understanding of the AIT resources and their applications, two matrices were developed. An AIT Functional Capability Matrix was developed to identify and assess the capabilities of the AIT resources. An AIT Card Application Matrix was developed to identify the automation of various applications with these technologies.

The matrices can assist system designers, system integrators, information system management personnel, users, and consumers of AIT resources understand the functional capabilities and the applications of these technologies in a concise format. The matrices can be used for selection and acquisition of AIT systems and to track and address migration of the AIT systems throughout their life cycles.

TABLE OF CONTENTS

ACKNOWLEDGEMENT

I. INTRODUCTION

A. BACKGROUND

Acquiring and managing goods and services has been around for several thousands of years. In the beginning, goods and services were managed and traded for goods and services. When humans finally got serious about trade and how to account for trading concerns, humans created metal ingots, which were assigned some value. Around 650 B.C. in Asia Minor, coins were developed and used in acquiring goods and services. In France, during the eighteenth century, paper money made its way into the trading environment. And the twentieth century was marked with the creation of the credit card by the United States during the 1950s to further facilitate goods and services transactions. [BELS93] In order to acquire and manage goods and services more effectively and efficiently, space and computer technologies, which spurred the "Information Age," provided the means to automate manual manufacturing, management, and acquisition of data collection processes. Manual data collection processes, possessed with keying mistakes, missing data, inefficient information distribution and delays, affected the efficiency and effectiveness of organizational operations. These inefficiencies cost organizations many billions of dollars in lost sales, created unnecessary and wasteful business expenses [TUTT94], and further heightened the awareness of executive and management personnel that changes must occur for the organization to succeed. Automation of these processes seemed to be the optimal solution and the means and technologies were available to make these changes.

With the movement to automate various functions and applications, automated data collection (ADC) technology, also know as automatic identification technology (AIT), and systems were identified and developed to accurately and rapidly capture, collect, and store data. These technologies emerged in a variety of forms and media for various uses. All the AIT resources have the same purpose, to accurately and rapidly capture data, but the difference of these technologies is the method used to capture and process the data. The major AIT resources that have been applied in some form to automate data collection applications are magnetic ink and optical character recognition (MICR and OCR,

respectively), bar code, magnetic stripe, radio frequency (RF), biometric and voice data collection, machine vision, optical (e.g., laser) memory, and integrated circuit "IC" card technologies. [INDU92] The "IC" card technology consists of smart card, IC memory card, and super smart card technology. The Personal Computer Memory Card International Association (PCMCIA) card is an IC memory card technology. [SEID94, p. 207]

The various AIT resources are being used in the private and public sectors and the government services. These technologies are making their way more and more into our every day lives. The use of these card technologies have affected how we do things and how we manage and acquire goods and services. Application and use of these technologies has created the need for organizations to revaluate their current business operations and to reengineer processes to become more efficient and effective at meeting the customer needs. The noted benefits of using these technologies in automating applications and systems are best realized when information is integrated and shared among individuals throughout the whole operation rather than used to address a specific need in a single part of an operation. [INDU92]

New ways of using these card technologies are being developed every day. With the additional capability of having multiple card technologies on one card, called "Hybrid" cards, these cards will have greater potential for future use in many applications, with their use only limited by the creators' imagination. The world of card technologies is here and it is a matter of time to see how the evolution of these technologies will change the way we presently conduct our day-to-day business as we progress in this "Information Age."

B.   OBJECTIVE

The objective of this thesis is to identify the various AIT resources and their functional characteristics, identify which AIT resources have been applied in a card format and the associated application, and to develop tools to assist information systems personnel, system designers, system integrators, decision makers, users and consumers in the use of these AIT resources. This study will require an extensive literature search of the available AIT resources and their applications, an understanding of the functional

2

capabilities of each technology, and the development of some evaluation system to facilitate the use of this information.

AIT resources are being used in many applications to automate, collect and distribute digitized information to various data collection and processing locations. The research of the AIT resources yielded a wealth of available information, but an effective and efficient means of identifying and using this information was not identified. In order to understand and keep abreast of how these technologies can be used in this "Information Age," personnel associated with and/or interested in automated data collection technologies should be knowledgeable of what these technologies are and how they can be effectively implemented to meet information resource needs.

C.   SCOPE AND METHODOLOGY

The scope of this thesis research is to identify the AIT resources used for automated data collection, identify the characteristics of the AIT resources, identify various AIT applications, and develop tools to facilitate understanding and implementation of AIT resources.

The methodology used in this thesis research consists of the following:

- conduct an extensive literature search of books, magazine articles, CD-ROM systems, and other library information services describing AIT resources;

- contact manufacturers and government organizations producing, using, and researching AIT resources to obtain AIT standards, specifications, product and application information;

- review various studies, reports and other documentation related to AIT program management issues;

- confer with AIT experts on the accuracy and appropriateness of the AIT information and equipment operation;

- attend two AIT card technologies conferences, one sponsored by CardTech/ SecurTech, Incorporated and one sponsored by the Smart Card Forum; and

• attend one "one-card campus" application conference sponsored by the National Association of College Auxiliary Services (NACAS).

Characteristics, technology specifications, applications and general cost information for each AIT card technology will be gathered from various sources and will be used as the primary data source for this study. AIT resource performance information will be accepted as provided or will be based on discussions with AIT experts and use of AIT equipment to verify the accuracy of research. This research study did not focus on total card system costs, but on various functional characteristic features of each AIT card technology. Total card systems costs will vary based on the application, the chosen AIT card technology, and the type of system integration required for the specific application. Therefore, total card system cost was not a major focus of this thesis.

D.   ORGANIZATION OF THE THESIS

The thesis is organized into seven chapters. This chapter provides the introduction, objective, scope and methodology used to conduct the research on the AIT card technologies. Chapter II provides a background on the various AIT resources and their functional characteristics. Chapter III identifies uses of AIT card technologies in various applications to establish a basis for understanding how these technologies can and have been applied to meet user needs. Chapter IV identifies the development and application of a functional capability matrix and an application matrix to assist integrators, managers, and users of these technologies. Chapter V identifies security issues related to the various card technologies. Chapter VI identifies a selection and acquisition strategy to use when considering AIT resources for automating a data collection application. Chapter VII covers conclusions and future research recommendations derived from conducting this thesis study.

II. AUTOMATIC IDENTIFICATION TECHNOLOGY (AIT)

A.   DEFINITION OF CARD TECHNOLOGY FOR AIT APPLICATIONS

In order to understand what is meant by the term "card technology," a review of the two words "card" and "technology" is appropriate. A "card" is "a rectangular paper or plastic medium used to show information relating to its issuer, user, and acceptors. It may include appropriate control information such as dates and services for which it is used." [SVIG87, p. 195] Various other media for cards have been used, which include cardboard, pasteboard, and optical media. "Technology" is defined in Webster's II as "the application of science especially to industrial or commercial objectives, the body of knowledge available to a civilization that is of use in fashioning implements, practicing manual arts and skills, and extracting or collecting materials." [WEBS88, p. 1188] With the combination of the two definitions, "card technology" can be defined as "the application of science to the industrial or commercial objective of using a rectangular medium (paper, cardboard, pasteboard, plastic, etc.) to show information relating to its issuer, user, and acceptors, e.g., name, dates, services and other information used for identification or classification."

From this understanding of the term "card technology," one can understand the concept that card technologies can originate from a variety of sources using a variety of formats and media. The physical card format typically meets the International Organization for Standards (ISO) card standards, ISO 7810, which defines the physical characteristics of the identification card or standard credit card. The physical characteristics of identification cards include the card materials, construction, characteristics, and dimensions of the card. The standard card dimensions are length of 3.375 inches, width of 2.125 inches, and thickness of 0.030 inches. [HAEU93] Figure 2.1 is an example of the plastic card meeting ISO standards. In addition to the card standard, each AIT card technology has additional draft and/or published standards for their specific characteristics, design and implementation features.
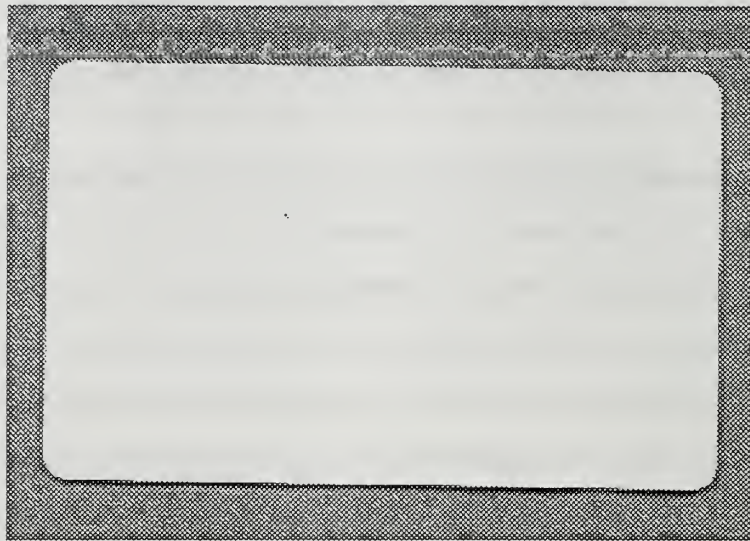
Figure 2.1: Plastic Card

The major AIT resources that have been applied in some form to automate data collection applications are magnetic ink and optical character recognition (MICR and OCR, respectively), bar code, magnetic stripe, RF, biometric and voice data collection, machine vision, optical (e.g., laser) memory, and integrated circuit "IC" card technologies. [INDU92] The "IC" card technology consists of the smart card, IC memory card, and super smart card technology. The Personal Computer Memory Card International Association (PCMCIA) card is an IC memory card technology. [SEID94, p. 207] Figure 2.2 identifies these AIT resources.

From the list of AIT resources, the media that can store the digital data in some form on a standard credit-size card are identified as AIT card technology media. These technologies include bar code, magnetic stripe, RF, optical, and integrated circuit or "IC" cards. The features of these technologies establish the base to which data can be written, read, and stored, and where enhancing technologies can be applied to add more desirable features to the card.

6

```
                        AIT RESOURCES

┌──────┬─────────┬──────────────┬──────┬────────┬─────────┬──────────┬─────────┐
│MICR/ │Bar Code │Magnetic Stripe│RF/ID │Optical │IC Cards │Biometric/│Machine  │
│OCR   │         │              │      │        │         │Voice Data│Vision   │
└──────┴─────────┴──────────────┴──────┴────────┴────┬────┴──────────┴─────────┘
                                          ┌──────────┼──────────┐
                                       ┌──────┐  ┌───────┐  ┌─────────┐
                                       │Smart │  │Super  │  │IC Memory│
                                       │Card  │  │Smart  │  │Card     │
                                       │      │  │Card   │  │         │
                                       └──────┘  └───────┘  └────┬────┘
                                                            ┌─────────┐
                                                            │ PCMCIA  │
                                                            └─────────┘
```
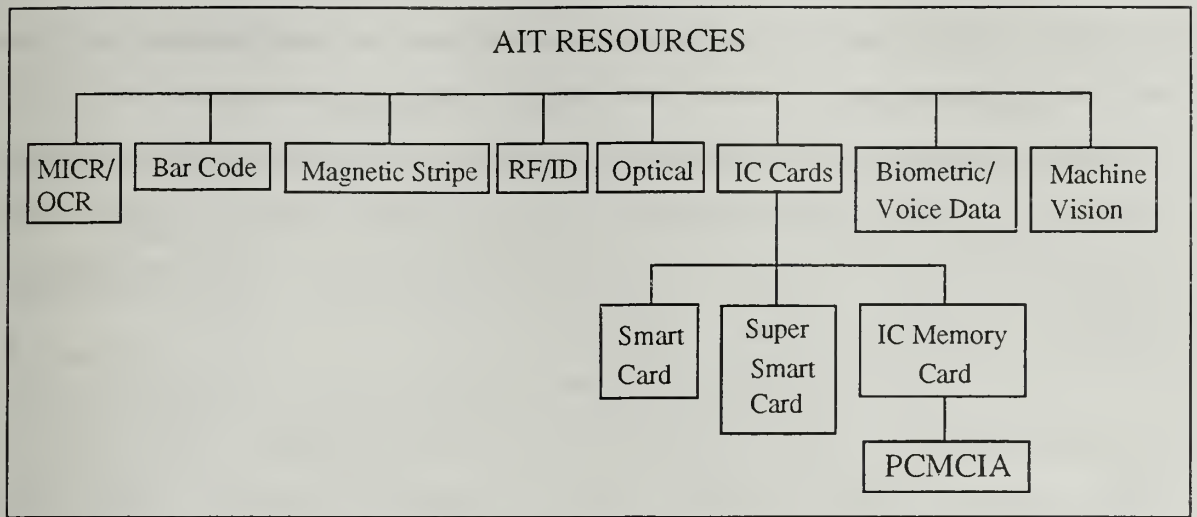
Figure 2.2: AIT Resources [INDU92] [SEID94, p. 207]

Biometric and voice data collection, and machine vision are considered enhancing technologies to the card technologies. These technologies are considered enhancing technologies because they are not card media themselves, they are data digitized from some form to be used for their value-added features to the basic card media. Examples of biometric technologies include, and are not limited to, hand geometry, fingerprints, thumbprints, retinal scan, and iris scan. Voice recognition consists of digitized voice patterns. The biometric and voice data is captured through various mechanical means and converted to digitized data. The data is transferred to the card to be used for identification, signature or user authentication. Machine vision uses mechanical systems to read other AIT resources, such as bar codes, and transmits this data to the integrating system to make further logic decisions for operational processes.

Magnetic Ink Character Recognition (MICR) and Optical Character Recognition (OCR) technologies are effectively used for printed or text media and they have been in use for many years. MICR technology has been effectively used in the banking system for check identification for over 20 years. OCR technology, which is comprised of "stylized" fonts, has been effectively used in applications which required high character density,

human readability, and where type-written or computer-printer material must be read. [DAVI91, p. 24] Through the literature search and in correspondence with card technologies experts, it is not evident that these technologies are being used as a media in the card technology area. This is not to say they can not be used for this purpose. For issues relating to this thesis, these technologies will be discussed to inform the reader of their availability, but they will not be included as a key technologies in the functionality or application matrices for AIT card technologies.

The following sections in this chapter identify the card technologies and their functional capabilities. The information for the AIT card technologies was gathered from various resources to include literature searches, conference attendance, correspondence and communication with vendors and "expert" personnel in card technology research, development and application environments.

B.   BAR CODE TECHNOLOGY

Bar code technology had its beginning in the late 1940s by Joe Woodland and Berny Silver, who were researching technical solutions for use in the automatic pricing of grocery products at the checkout stand. Various approaches were pursued which led to the development and filing of U.S. Patent 2,612,994 in 1949 for a bull's-eye code. The bull's-eye code consisted of a circular printed pattern, resembling a miniature archery target, of bars and spaces curved into a circular form. This technology was a precursor to bar code technology. Bar code technology research was continued, and in the late 1950s and early 1960s, other forms of bar code technology began to emerge. [PALM91, p. 11]

1. Characteristics

A bar code consists of a pattern of bars and spaces of various widths that represent letters, digits, and punctuation symbols. The bars and spaces are arranged in a "symbology". [DAVI91, p. 12] There are several symbologies, which include Universal Product Code (UPC), European Article-Numbering (EAN) system, Japanese Article-Numbering (JAN) system, Interleave 2 of 5, Codabar, Code 11, Code 39, Code 49, Code 93, Code 128, Code 16K, 2 of 5 Code, Plessey Code (Pulse Width Modulated), Matrix 2 of

5, Nixdorf Code, Delta Distance A, Ames Code, Postnet, Codablock, and far lesser known symbologies applied by individual sponsored companies which include AGES, AS-6, AS-10, Calra Code, F2F, Fujitu, Norand (version of F2F), RTC, Toshiba, Telpen, PDF 417, Vericode, Datacode, [PALM91, pp. 21-59] Identification Matrix and Code 1. [ZAGU94]

Many of the bar code symbologies have been successfully applied in various applications. The UPC and UPC/EAN bar codes have been successfully used in the retail market place, specifically the supermarket industry where the bar codes are designed to uniquely identify a product and its manufacturer. A high degree of data security has been demonstrated with UPC/EAN. Code 39, also known as Code 3 of 9, is a discrete, bidirectional, alphanumeric symbology of various lengths with self-checking properties that offers a high degree of data security. This symbology has become the de facto non-retail symbology [PALM91, p. 31] particularly in industrial, medical and government applications. Interleaved 2 of 5 is a self-checking, high density, numeric symbology adopted by the Uniform Council of Code. [DAVI91, p. 12] This symbology is mainly used in the distribution industry [PALM91, p. 25] and is popular for use on the outside of the shipping containers, for warehouse inventory handling, and in heavy industrial applications. Code 93 and Code 128 are high density alphanumeric symbologies that offer high data security [DAVI91, p. 12], can be of various lengths, and are used in retail distribution applications. [PALM91, pp. 35, 38] PDF 417, 16K, Codablock, and Code 49 are "stacked" symbologies. These stacked symbologies have a fixed width format with "two dimensional" stacked rows of bar codes and high-density data encodation. [DAVI91, p. 12] Codabar is a discrete, self-checking symbology with 16 characters in a set. It is mainly used in blood banks, libraries, and air parcel express applications. [PALM91, p. 28] And lastly, matrix codes, such as Vericode and Datacode, are bar codes that provide high-density data storage. [DAVI91, p. 12] Figure 2.3 is an example of bar code technology applied to a standard credit-size card. The bar code on the top is an example of Code 39, a one dimensional (1D) or "linear" bar code, and the bar code on the bottom is an example of PDF 417, a two dimensional (2D) bar code.
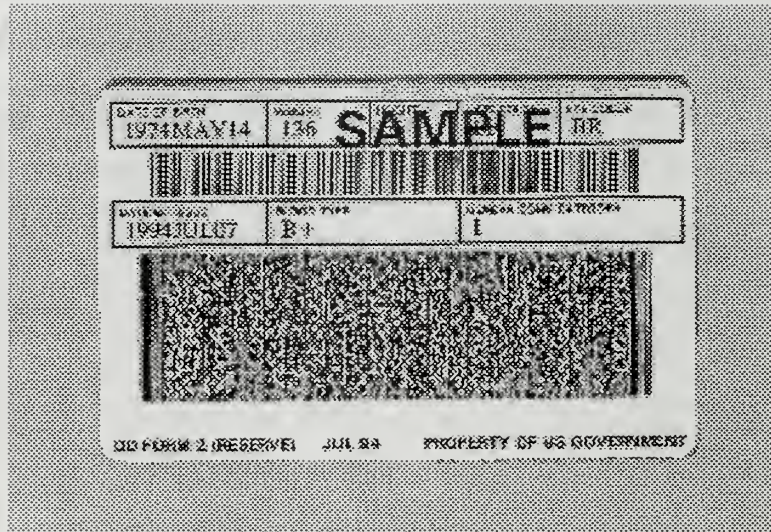
Figure 2.3: Bar Code Technology

The bar code is used to identify an item or regulate its movement. In use, a bar code is scanned by a beam of light (typically laser) from a scanning reader mechanism with the dark bars absorbing the light and the spaces reflecting the light back into the scanner. The light fluctuations are transformed into electrical impulses in the scanner, mimicking the bar and space pattern of the bar code. The electrical impulses are transmitted to a decoder which uses mathematical algorithms to translate the impulses into a binary code. The encoded data is then transmitted to a personal computer (PC), a controller or a host computer system for storage and use. Various decoders exist and may be integrated with or external to the scanning devices. [DAVI91, p. 12]

All bar codes have several similar components. They have a clear space, called a "quiet zone," before and after the code; specific start and stop patterns which indicates the beginning and ending of the code; and special check characters (mandatory in some codes) which verify the accuracy of the encoded information through a mathematical check. Bar

codes, as well as other AIT resources, can contain data identifiers. The data identifiers are code prefixes that identify the meaning or intended use of the data that follows the code. [DAVI91, p. 13].

The data capacity of each bar code is based on the particular symbology used and the encoding scheme. For example, there are three versions of UPC bar code: Version A consists of 12 digits, Version E consists of 6 digits, and Version D is variable length, which is seldom used; EAN bar code has two versions: EAN-13 consists of 13 digits and EAN-8 consists of 8 digits; Interleave 2 of 5 is used for fixed length applications and is typically characterize as 18 characters per inch; Codabar has 16 characters in a set; Rationalized Codabar has 20 characters; and Code 39 consists of 9 elements, to list a few. [PALM91, pp. 21-34] The recommended data storage capacity of Code 39 for military use is a maximum of 32 characters. [MIL-STD-1189B, p. 13] The PDF 417 bar code has data storage capability of 2725 maximum digits per symbol by converting numeric strings from base 10 to base 900. [ITKI92] In general, 2D bar codes, like PDF 417, have more data storage capability than 1D bar codes, like Code 39 (over 2K versus 32 bytes). In comparison to other AIT card technologies, data storage capacity of a bar code is limited and can affect the use of this technology in various AIT card applications.

Two important pieces of equipment required for all bar code systems are the bar code generating and printing equipment and the scanning equipment. [DAVI91, p. 12] The bar code can be generated and printed directly on the end item or it can be applied to a substrate (label, tag, page, form, or conventional packaging material) that will be applied to the item. The label or tag can be metal or fabric. [PALM91, pp. 134-135] A metal label or tag can be riveted to the item; it is the most durable and the most costly medium to use. The fabric label substrates are exclusively "peel and stick," with the adhesive already applied to the label. Proper cleaning of the item must occur to ensure the fabric label will remain in place. Fabric labels are susceptible to environmental conditions, such as fading from light sources, burning, and chemical reaction. [MIL-L-61002] These labels must be verified at periodic intervals to ensure readability. When readability can no longer be achieved, the bar code must be replaced. [LAIR94]

The bar code label can be manufactured by an outside vendor or printed on site (in house) using various techniques and a variety of printers. The various printing techniques for preprinted labels include electrophotography (lasers), flexography, hot stamping, inking wheel, ion deposition, laser etching, letterpress, offset lithography, photocomposition, or rotogravure. [PALM91, p. 109] Printers used for bar codes include dot-matrix and other impact printers; ink-jet printers; thermal, thermal label, and thermal transfer printers; ion deposition printers; xerographic printers; magnetographic printers; and electrophotography (laser) printers. [PALM91, pp. 117-130] The technique and printer used should depend on the specific bar code application.

Various scanning equipment exist for reading a bar code symbology. The scanning equipment uses visible and infrared light to read the bar code. Some scanning equipment require contact with the bar code or label and some scanning equipment can read the bar code from various distances, up to several feet. Scanner systems can be hand-held or stationary. The beam of light in the scanner system can be fixed or moving. The scanner system used should be matched with the specific bar code application. [DAVI91, p. 12]

Bar code standards have been developed and are an essential factor for their use. There are three types of bar code standards; symbology, application, and print quality standards. The symbology standard specifies the bar code structure by defining the particular arrangement of bars and spaces of various widths that make up the bar code symbol. Symbology standards have been written by various groups for various symbologies. For example, American National Standard Institute (ANSI) published standard MH10.8M-1983 for Interleave 2 of 5, Code 39, and the Traditional Codabar symbologies, and the United States Department of Defense (DoD) published Military Standard 1189B (MIL-STD-1189B) for Code 39 symbology. [PALM91, pp. 61-63] The application standard specifies information for bar code use in a particular industry or application. It defines the symbology standard, what information is encoded, and the labeling requirements, including placement of the symbol on the labeled item. Application standards have been written by various groups. For example, United States Department of Defense Military Standard 129H (MIL-STD-129H) defines product marking for shipment

and storage and specifies the required bar code data and human-readable information. [PALM91, p. 64] Print quality standards arose from the resolution dependence of the scanner to read the bar code symbology. They specify the size and shape of the measuring aperture of the scanning equipment. [PALM91, p. 66] MH10.8M-1983, published by ANSI, identifies some print quality standards. [PALM91, p. 63]

With many identified types of published standards, it is important for a bar code to conform to the system specifications and be verified before it enters the data flow process. The verification is achieved with verification or analyzer-type equipment that meets the particular bar code system requirements. [DAVI91, p. 13]

Bar code technology can provide accurate and timely data collection for simple or sophisticated management systems at a reasonable cost. An important feature for accurate and timely data collection is successful scanning of the bar code to yield a high first-time read rate. Therefore, the bar code should be readable with adequate contrast between the bar code and the medium where it is printed. [DAVI91, p. 12] Cost of the bar code when applied to a credit-sized card is $0.10 to $0.25 per card. [INFO94, p. 24] Use of bar code technology can be an economical, cost saving solution to increase accuracy and productivity, which will improve the business operation. [DAVI91, p. 12]

2. Applications

Bar code technology is used in various applications and has found wide spread use in clean environments where there is minimum interference from rain, snow, ice, dust, mists, etc. [MILS93, p. 230] A majority of bar code use is in logistics applications, for inventory control and product identification. Other application areas include accounting and record keeping systems, inventory and product tracking, personal identification, library system, check cashing, [INFO94, p. 23] campus card, benefit delivery (food stamp), debiting and personnel management, toll collection, [FMS90, p. 255] access control, check-in/check-out, employee card, time and attendance recording, document tracking, monitoring work in progress, order entry, point-of-sale (POS) operations, quality control, route management, shipping and receiving, sortation, warehousing, in health/medical systems for patient care aids from tracking medicinal usage to patient billing, [DAVI91, p.

12] and manufacturing and distribution of health care products. [PALM91, p. 205] This is just a brief list of applications, which scratches the surface of where and how bar code technology is being applied. Other applications can be identified in various trade publications, and by manufacturers and distributors of bar code technologies. Bar code technology can have limitations with regard to distance, speed, and orientation of the bar code relative to the reading device, [MILS93, p. 230] which is important when selecting this AIT resource for specific applications.

3. Strength

The main strength of the bar code is it is a simple and proven technology. It is easy to create or acquire from vendor sources and it requires interaction with equipment that has few moving parts. Other strengths include: it can be printed on a variety of media; it operates passively, there are no write mechanisms required for the use of this technology once the initial identification has been established (e.g., write once, read many (WORM) technology); there is a wide range of bar code symbologies to use with various scanning technologies available to read the bar code and transmit it into a usable format; it is not susceptible to electromagnetic interference; the data is secure based on the symbology used and the specific error rate identified with the symbology [PALM91, p. 153]; and the implementation and maintenance cost is low when it is compared to other AIT card technologies (e.g., smart card and optical card). [INFO94, p. 24] Bar coding is a good technology to use in application areas that require a central database for storage and retrieval of information. [INFO94, p. 23]

4. Weakness

In general, the main weakness of the bar code technology is security of the bar code itself; the bar code can be easily duplicated or counterfeited. [INFO94, p. 23] Other weaknesses of bar code technology include limited data storage capability based on the bar code symbology used when compared to other AIT card technology media (e.g., smart card, optical card); limited flexibility for its various uses; [MILS93, p. 230] and it is susceptible to environmental factors inherited from the media to which it is written. For the

purpose of this thesis, the application of the bar code on plastic, paper, or other fabric media makes it susceptible to the environmental conditions of fading, melting, burning, etc., and it can be affected by chemicals. [INFO94, p. 23] Even though there are no write mechanisms, the labels must be verified periodically to ensure readability. When label readability is no longer achieved, the bar code must be replaced. [LAIR94] This affects the usefulness of the bar code label in some locations and in some applications.

C.   MAGNETIC STRIPE TECHNOLOGY

Magnetic stripe technology has been in use as a card technology since the late 1960s. Its first use was in the financial transaction card (FTC) market. As the capabilities of the technology and its use became known, the applications of this card technology was adapted to other areas and its use continues to grow. [SVIG87, p. 165]

1. Characteristics

The magnetic stripe technology uses a magnetic field of some medium to record magnetic flux reversals. Information is coded electronically onto this layer of magnetic material called a magnetic stripe. The storage capability of the magnetic stripe is based on its coercivity,[1] which is the magnetic "retention value" of different ferrous oxide materials. Low coercivity (LoCo) is based on iron oxide media and high coercivity (HiCo) is based on barium ferrite media. [KUTC92] The higher coercivity of the magnetic material used for the magnetic stripe will result in more permanent information storage. Therefore, use of a high coercivity magnetic stripe material will improve security and lower the risk of accidental erasure of the card data. [MOS92, pp. 57-58]

The information on the magnetic stripe is transmitted with an encoder/decoder (writer/reader) system. The encoder/decoder system generally requires the magnetic stripe to be moved under the reading or recording head for the magnetic stripe contents to be

---

[1] Coercivity of the material relates to the required amount of energy to change the magnetic state of the material. It is measured in oersted. [DREI92, p. 150]

written, read, erased, altered, or rewritten. [SVIG87, p. 36] In use, the data, e.g., numbers and letters, is transmitted to the encoder, which creates flux reversals on the magnetic stripe. The decoder, or card reader, reads the flux reversal of the magnetic stripe and translates it for processing by a computer or terminal equipment. [DAVI91, p. 22]

Magnetic stripe technology has been standardized by the ISO as ISO 3885 and by the American National Standards Committee (ANSC) as ANSC X3B10 for its features and use. Table 1 identifies the various segments of the magnetic stripe card standards. These standards fit into two general categories: physical and application. The physical standards identify the recording track locations, the data densities, the magnetic recording qualities, and the encoding methods. The application standards define the format and data content of the magnetic stripe for its various uses. Implementation of the magnetic stripe standards are mandatory in certain applications, such as financial systems, but can be voluntary for other applications. [DAVI91, p. 22]

Magnetic stripe technology has many features to support its use for various applications. The standard magnetic oxide stripe thickness is approximately .0005 inches and can be attached to the front or back of a paper or plastic card. It allows the storage of data in a small area that is specific to the application standard. [MOS92, p. 64] A single

---

Physical card (ISO 3885/00)
Recording technique - embossing (ISO 3885/10)
Recording technique - magnetic (ISO 3885/11)
Recording technique - location of embossed characters (ISO 3885/20)
Location of read-only magnetic tracks (tracks 1 and 2) (ISO 3885/30)
Location of read-write magnetic track (track 3) (ISO 3885/40)
Numbering system and registration procedure for issuer identifiers (ISO 3885/70)
Financial transaction card, track 1 and 2 content (ISO 3885/80)
 Banking - only track 3 content (ISO 4909)

Table 1.   Magnetic Stripe Card Standards [SVIG87, p. 23]

16

magnetic stripe can consist of one or several tracks to store recorded data on the card. [DAVI91, p. 22] Figure 2.3 is an example of magnetic stripe technology applied to a standard credit-size card. The magnetic stripe data format and recording information is identified in Table 2. [SVIG87, p. 26] With the read/write capabilities, security features can be implemented with magnetic stripe technology to include the use of personal identification numbers (PINs). [SVIG87, p. 12]
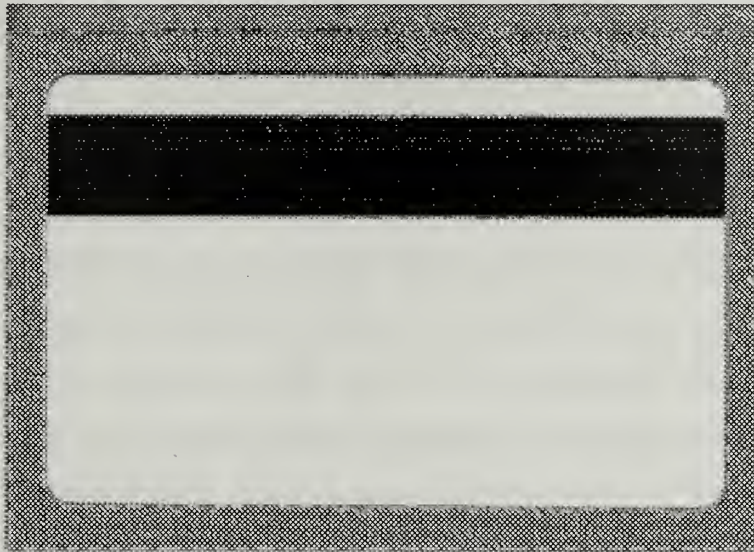
Figure 2.3: Example of Magnetic Stripe Technology

	Recording Density (bits per inch)	Character Configuration (bits per character including parity)	Information Content
Track 1	210 bpi	7 bits	79 alphanumeric characters
Track 2	75 bpi	5 bits	40 numeric characters
Track 3	210 bpi	5 bits	107 numeric characters

Table 2: Magnetic Stripe Card Data Format [SVIG87, p. 26]

The magnetic stripe card in use today is typically an embossed plastic card with read capabilities that can be employed at a reasonable cost. In general, low density magnetic stripe cards have data storage capability of 150 characters and cost $0.50 to $1.00 per card; high density magnetic stripe cards have data storage capability of 475-500 characters and cost $0.85 to $1.50 per card. [INFO94, p. 24] The card is mainly used with a centralized database in passive (read-only) operations vice being used for interactive operations (read/write) where other AIT card media are better suited. [SVIG87, p. 27] In addition, the remaining space on the magnetic stripe card is available for other uses, such as photographs, bar codes, fingerprints, and logos. [SVIG87, p. 37]

2. Applications

Magnetic stripe technology can be applied in various applications. It has been effectively use in card applications systems to include campus card, personnel management, time and attendance, vehicle registration, licensing, financial management, benefit delivery/disbursement of government benefits (funds, food stamps and services), school lunch programs, access control, airport security, fuels management, [FMS90, pp. 255-257] in credit and debit card applications for automatic teller machines (ATMs) and point-of-sales (POS) terminals, inventory tracking, manufacturing process control, transit fare collection, personnel identification, access to amusement parks and games, vending, and as stored value cards. Magnetic stripe technology has been popular for use in security applications. [DAVI91, p. 22]

A valuable feature of magnetic stripe technology is it can store "cash value" for use in debit card applications. For debit card applications, the card can be encoded with a specific monetary amount leading to its purchase before its use. The card is then used to purchase goods or services with the "cash value" of the card magnetically decremented for each use. Other terms used for the debit card are POS or prepaid cash cards. Examples of debit card application are for student meal programs, telephone toll call systems, transit (bridge, tunnel, road fees) systems, mass-transit tickets, vending machines, and video clubs. [DAVI91, p. 22]

3. Strength

The main strengths of magnetic stripe technology are that it is a proven technology, ISO standards have been developed and implemented, the infrastructure is well established throughout the United States and the world for its use, and it has security capability with the use of PIN authentication. Therefore it is considered a low risk technology. Other strengths include magnetic stripe cards can consist of multiple tracks to use in various application areas, the tracks can be low density or high density, and it can store a certain amount of data.

Magnetic stripe card technology can be acquired through many vendors. [INFO94, p. 22] With the support of many vendors, the implementation and maintenance costs are low when compared to other AIT resources (e.g., smart card, optical card). The low cost and well established infrastructure are key elements that can drive automating various applications with this card technology. Due to its passive characteristics, magnetic stripe technology is mainly applied in areas that have a centralized database or access to a centralized database for additional information retrieval. [SVIG87, p. 27]

4. Weakness

Like bar code technology, the main weakness of magnetic stripe technology lies in the area of security. The magnetic stripe is magnetically volatile and it is relatively easy to alter or duplicate, making it extremely susceptible to fraudulent use. Other weaknesses include the limited recording density of the track, which limits its data storage capabilities; [INFO94, p. 24] the lack of logic capabilities for security control to read or change the content of the card when fraud is detected; and the lack of the local ability to journalize security functions (e.g., audit trail capabilities). [SVIG87, p. 172] Due to its passive operation and limited data storage capabilities, its application is best suited for centralized database system vice distributed database systems. [SVIG87, p. 166]

Some technical weaknesses of the magnetic stripe card result from the mechanical aspects associated with this card technology. The technology required to read the card is more mechanical and serial in nature. Therefore, it is susceptible to more mechanical

hardware failures compared to other card technologies. In addition, the protective overlays on the magnetic stripe require extra flux density in the head gap of the read/write mechanism which can affect card use. [MOS92, pp. 57-58]

The magnetic stripe card technology is susceptible to environmental factors, which include temperature extremes, chemicals, and other external agents or magnetic sources. The magnetic stripe card is sensitive to extreme temperature variation inherited from the medium to which it is written (e.g., paper or plastic). It can be affected by chemicals which can damage the protective covering of the medium and the magnetic stripe. And the magnetic stripe can be affected by bending the card, scratches on the magnetic stripe, dirt particles on the card medium or in the reader/writer mechanism, and contact with other magnetic material. [SVIG87, pp. 31-33]

D.   RADIO FREQUENCY IDENTIFICATION (RF/ID) TECHNOLOGY

Radio frequency identification (RF/ID) technology has been used for automatic data collection since World War II. [TUTT94, p. 361] The driving force behind the use of radio frequency technology was to automate item identification in situations or environments where automated optical identification (i.e. bar code technology) was inadequate, such as interference from rain, snow, ice, dust, mists, etc. In addition, use of radio waves do not have the serious limitations that other technologies have with regard to the distance, speed, and their orientation relative to the read/write device. [MILS93, p. 230]

1. Characteristics

RF/ID technology systems have non-contact readability features by using radio frequency transmissions. Radio transmitters and receivers pass electronic information using radio frequency to and from an electronic card or tag to a computer system for storage, retrieval and use. The electronic card or tag is programmed with unique information and attached to an object for identification or tracking. The information is read or written by a "reader" or "interrogator" system. [DAVI91, p. 30] Since RF/ID technology

features apply to both card and tag media form, this author has chosen to use the term "tag" to address the full capabilities of this technology. Figure 2.5 is a example of an RF tag. [SAVI94]

An effective RF/ID system requires five components: the tag, the interrogator, the host computer system, the software (including the required data communication protocol), and an RF wave (frequency component) transmitter. Some of these components come in a variety of shapes and sizes and can be placed practically anywhere for use. [SABE94]. Each of these components has specific features that should be considered when implementing a RF/ID system. [MILS93, p. 235]

The electronic tag has design characteristics which include a variety of forms, types, frequencies, memory capacities and options. RF/ID card/tag technology come in two forms: read/only or read/write. Read/only systems typically support passive operations, whereas read/write systems support interactive operations between the media and the
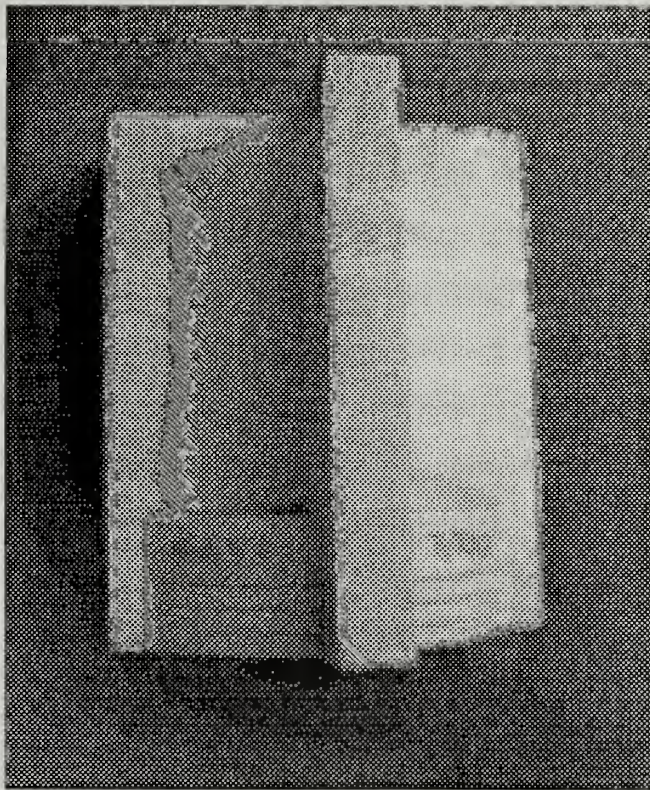
Figure 2.5: Example of RF tag. [SAVI94]

host system. The read/write systems can "write" to the tag by adding new information or changing existing information on the tag. Tags can be of two types, a passive type where the power comes from the interrogating or reading transmitter or an active type which has an on-board power source, e.g., a battery. The tag can support various frequency range capabilities of low, medium, and high [DAVI91, p. 30], and they can be procured based on the desired memory storage capacity. The tag may come with a variety of options and in a variety of sizes. [INFO94, p. 19]

The two types of RF tag technologies have different operational characteristics which arise from the different power requirements. The passive or reflective type RF tag technology draws its transmission power from an incoming energy signal from the interrogating transmitter. The active type RF tag technology is a two-way communication system that has its own power source, usually a lithium battery, and therefore relies less on the power of the interrogator. The lithium battery has an useful life of approximately 4 years and depends on the number of interrogation cycles. [REBO94] In operation, the central node or host computer sends out commands through the low power interrogator unit, either automatically or manually. Through two-way communication, the interrogator identifies the tags within the specific interrogator read range, and the exchange of information to and from the tags occurs. The interrogator unit can operate omni-directionally and can communicate with the tag regardless of tag location or orientation on the object. The interrogator unit can be commanded to communicate with the tag individually or to all of the tags simultaneously. The interrogator can be programmed to automatically query the tags at any time of the day. Successful communications, with handshaking and acknowledgment, can be assured by using various diversity schemes and multiple antennas to minimize interference. Thirty RF/ID tags per second can be processed by some interrogator units. [MILS93, pp. 232, 236]

RF/ID card or tag have various memory capacity and associated cost. The RF/ID tag's memory size capability ranges from 8 bytes (characters) [INFO94, p. 19] to 128KB [VOSS94, p. 390] of programmable read/write memory. Currently, the tag's non-volatile[2] memory sizes are from 128 bytes to 128KB. [VOSS94, p. 396][DOD94] The best systems

are designed with the tag maintaining all the required information about the tagged item in the tag's own data base. This action assures the on-site user that they have the necessary information locally available and they do not need to rely on the accessibility or the completeness of the central database. In addition, it is important the system be established to store the data on the tag in a manner that it may be changed remotely through the host PC or the hand-held interrogator. [MILS93, pp. 232-233] The RF tag can costs as low as $5 to $20 with data storage capacity of up to 200 bits [HADD93, p. 389], $100 to $125 for data storage capacity of 8KB [INFO94, p. 24], and up to $190 for data storage capacity of 128KB. [DOD94]

The tag may come with a variety of options and sizes. The tag can include output wires or I/O ports to interact with electromagnetic actuating devices, direction finding devices, humidity and temperature sensors, optical fiber security sensors, and liquid crystal displays to allow manual reading of the memory contents of the tag. [MILS93, p. 236] The tag can come in various physical sizes, shapes, and configurations. [INFO94, p. 19] The main sizes are 2"x3"x1" and 4"x5"x1". They can be attached to an object by various methods, such as double sided tape, velcro, bolts, and glue. The tags can have an audio beeper for use in location finding. [MILS93, p. 236]

RF tag technology system can operate in various frequency ranges. Low frequency tags are typically small in size, have short read/write ranges from less than an inch to a few feet, experience little environmental interference, are omni-directional, [DAVI91, p. 26] and are inexpensive. Low frequency tag systems are best applied in environments where bar code or other AIT systems are not feasible. These tags operate at less than 1 megahertz (MHz). [MILS93, p. 230] The mid-range (medium) frequency tags operate in the 2 MHz to 15 MHz range. [CUSH94, p. 350] High frequency tag systems are intended to add range and high speed read capability. These systems operated in the high frequency ranges (usually AMTECH operates at 915 MHz to 2.45 GHz with reflective tags [REBO94]),

---

[2] Non-volatile means that in the event of battery tag failure, the data content of the tag is still intact. [VOSS94, p. 396]

require high power transmitters, require the tag to be in the transmitter's line-of-sight within certain range limits, and read the tags one at a time. These systems can be a cost-effective solution for item identification in a harsh environment or in a stable environment where the item is always present in the same place and in the same sequential format to the interrogator. These systems required a robust computerized database to be link to the tag for rapid item identification. [MILS93, pp. 230-233]

The interrogator unit is an important component of any RF/ID system and the type selected should be based on the specific application and environmental conditions. The interrogator can be fixed and mounted on an elevated structure, or it can be portable and carried around by an individual. The fixed interrogator typically contains 64KB of internal memory and can be set up with antenna sensors to read the information as the tagged object passes through the interrogator. The interrogator may be connected to the host computer through a telephone cable on a RS-232 or RS-485 network or it may be connected through a stand-alone RF-link. The power may be supplied through a 110 or 220 volt plug or by a solar/battery unit (RF-link use). Interrogators can be networked together to support data communication throughout the RF/ID system. They are not restricted to a rigid line-of-site communication requirement, and they can cover various ranges, from a 50-80 foot range indoor to a 100-200 foot range outdoor. Some interrogator units can reach operational ranges of up to 800 feet. [MILS93, pp. 235- 236]

Frequency selection is a very important element in RF/ID system application and it drives many of the other system parameters that must be considered, such as regulatory compliance, data rate, power consumption, reliability, size, line-of-sight requirements, and cost. Use of various frequencies can require Federal Communication Commission (FCC) approval and require obtaining site licenses for each interrogator or tag site. This process can be time consuming, costly, and can cause the RF/ID system to be rigid with regard to the use of movable or portable interrogators. Some RF/ID systems can be used with a no-license status under certain circumstances. Many companies that develop RF tag products try to select a frequency which use the no-license status. The systems developed for no-license frequency bands still required FCC certification for compliance with FCC

regulations [MILS93, pp. 230-233] and National Telecommunications and Information Administration (NTIA) Annex K for military applications [REBO94]. The three frequency bands available for low power transmission are 260-470 MHz (UHF), 902-928 MHz (915 band), and 2400-2484 MHz (2450 band). The systems that use these frequency bands operate under Part 15 of the FCC. [MILS93, p. 233]

The trade-off issues that drive the frequency band selection in operational environments are interference, scattering, multi-path, antenna design, and cost. Interference occurs from signals that collide at the same frequency, destroying the signal integrity and the information content. Scattering created by conductive surfaces affects all RF radiation, which includes RF data transmissions. Multi-path signaling occurs when signals reflect off numerous surfaces and the reflected and non-reflected signals collide to cause destructive interference to the RF transmission. The antenna design should be based on the specific application. It can be direct or omni-directional to make the RF/ID tag extremely useful and cover the required operational area. Cost is based on the material used in the components of the system, e.g., silicon, gallium arsenide. Silicon components are typically used for low frequency systems; they do not process the signal fast enough to handle the high frequencies. The material of choice for high frequency system is gallium arsenide, which is more expensive. UHF has been noted as the frequency band of choice for RF/ID systems, with the antenna size being a major consideration in the design of the system. In addition to the antenna design for the chosen frequency range, the power requirement and the application environment of the transmitter and/or receiver should be addressed. Certain military applications (e.g., fuzed munitions) are extremely sensitive to low RF power levels and safety can become a major issue. [MILS93, p. 235]

The proposed RF interface draft standard for RF/ID systems is ANSI American Standard Committee (ASC) X3T6. It is a non-contact interface protocol for a radio frequency transponder and interrogator. The final test plan for the protocol is required to be approved as an American National Standard draft proposal (dpANS) by December 1994. The protocol will be available for use in business and military logistics applications. [CARN94]

Security features of this technology are very important. The tag has memory that can be divided into partitions. A password can be assigned to each partition to protect the data stored in the partition. Through the use of start and stop addresses within the partition, the host system can send commands through the interrogator to gain access to the specific locations on the tag. RF/ID tags are extremely accurate, with calculated error rates as low as 1 in 100 trillion, and are difficult to counterfeit. Strong magnetic fields cannot erase RF signals. [TUTT94, p. 361, 365]

Data can be collected using other AIT resources (e.g., bar code, IC card, and magnetic stripe card) [REBO94] and transmitted using radio frequency transmission devices, to various locations for data processing. The radio frequency systems associated with these activities are known as "radio frequency data communications (RF/DC)" system. RF/DC is the transmission of the real time information between the tags or terminals at the distance locations over a wireless RF/DC link to the host computer system. Instructions are transmitted directly to or from the terminal points, the tasks are completed, and the appropriate information is transmitted to the host computer for immediate record verification and update. Two types of RF transmissions or multiplexing are used for RF/DC: polling and contention. The polling system consists of each RF terminal being polled or queried in a specific sequence. The contention system consists of each RF terminal transmitting information based on channel availability; the terminal listens to an RF channel and ensures the channel is clear before transmission. This RF/DC activity provides an on-line, real-time communication link without the need for traditional wire transmission lines. [DAVI91, p. 26]

2. Applications

RF/ID can be effectively used in many application areas. [CUSH94, pp. 346-347] With various RF/ID technology read range capabilities and its operation with or without line-of-sight requirements, they can be effectively used in harsh environments, in places where it can be uncomfortable for humans, for remote monitoring, [TUTT94, p. 361] and where other contact or near-contact ID readers could be damaged or misaligned during read/write operation. For example, RF/ID has been effectively used in rugged industrial

and military environments which require the higher ranges to operate and transmit information [DAVI91, p. 30] and in areas which require monitoring of dangerous cargo conditions from various distances. Based on the various capabilities of this technology, RF/ID can be ideally suited for application in these environments. [TUTT94, p. 361]

RF/ID tags can be used on people, places, animals, and objects. Application areas include the use of tags for access control systems/security; personnel monitoring, tracking, and identification for time and attendance recording, visitor control, hospital/nursing home patient tracking and monitoring, and prisoner tracking; vehicle monitoring for automatic truck weighing, state fuel reporting, facility access, and automatic vehicle identification (AVI) for fuel dispensing, traffic flow monitoring, railroad car and truck tracking; in automotive applications to include stolen vehicle tracking, vehicle identification number (VIN) tags, tire identification; in automatic revenue collection systems to include toll fees, parking fees, transit fees, general consumer fees; in factory and warehouse operations, to include tool identification, inventory tracking, warranty tracking, pallet identification, security, canister identification, packaging, automatic storage and retrieval; parcel tracking for mail processing and airline baggage and sorting; retail applications to include POS price readings, on-shelf price verification, order entry, direct store delivery, and inventory control; in article surveillance for consumer perishables, high value consumer durables, libraries, museums, businesses, and video stores; animal identification applications to include livestock movement control, automatic weighing, feeding, milk production recording, slaughter house operation, animal testing and research data collection, and dairy cow breeding cycle optimization; refuse container identification and billing. [CUSH94, pp. 346-347] The RF/ID systems can be hand-held or secured to material-handling equipment or containers, such as forklifts, pallets, and shipping crates. The material-handling industry uses RF/DC for shipping, receiving, storage, retrieval, order picking, and pick-slot replenishment. In addition, it is used with other automatic identification technologies, such as bar code and optical card technologies. [DAVI91, p. 30] Tags can be used and commanded to signal a hard-wired output device, such as a solenoid, to be activated (e.g., to open or close a lock or a door). [MILS93, p. 232]

RF/ID technology systems can be linked to a Global Positioning Satellite (GPS) to collect data anywhere in the world, from a home-base station to any remote location. [TUTT94, p. 361] RF/ID technology has been extremely important for military operations. The military has been researching and testing the use of new long range RF/ID tags and high memory storage devices, such as optical memory cards, to identify containers at long distances (over 100 feet) and transmitting this information to centralized transmission points of the automated RF/ID system. With these RF/ID systems, the tag is placed on the outside of the container. The tag contains an identification container number and other important information, such as the origin, the destination and the container contents. The high memory storage device hold all the other pertinent manifest information. The tag is read or written to using a portable or fixed interrogator. The user at a port facility can locate the container by its number, query each container to identify its content, and redirected the container shipment, if required, with a minimum of effort. Therefore, the RF/ID tag can be viewed as an extension of the communication and data base system. [VOSS94, p. 390]

3. Strength

The major strengths of RF/ID technology are the greater placement flexibility of the interrogator (read/write device) and the tag compared to other card technologies (e.g., bar code, magnetic stripe, etc.), RF signals cannot be erased by strong magnetic fields, and it can be use in various environments with various line-of-sight requirements. The tag's readability is not affected by dirt, dust, paint and other opaque substances. It is a very functional media to use with various environmental conditions of snow, rain, fog, various temperature ranges (extreme hot or cold), for remote monitoring or in harsh environments and places where humans are uncomfortable. Non-metallic objects can come between the electronic tag and the reader without response interference. Other strengths of RF/ID technology include "on-the-fly" identification where the tagged object does not need to stop to be interactive with the interrogator or reader system. [DAVI91, p. 30] The RF/ID tag's read range is contingent upon the size, space, and obstacles that might interfere with the interactive operation of the radio frequency transmission. [INFO94, p. 19] RF/ID systems have been effectively used where bar code systems are not feasible. [MILS93, p.

230] RF/ID systems can have lower implementation and maintenance costs since these systems do not have moving parts for the read/write process, unlike magnetic stripe and some bar code systems. [REBO94] These systems are not as limited with regard to speed, distance and orientation of the RF/ID tag. RF systems can effectively communicate at high speeds between the RF system components. [MILS93, p. 230]

Other strengths include: RF/ID systems can operate without human intervention, unlike other AIT resources (e.g., magnetic stripe), and the logic capability for the tag's operation can be supplied through the host computer system. The data storage capability of an RF/ID tag is contingent on the size of the tag (up to 256 KB) in comparison to bar code or magnetic stripe card technology, which hold smaller amounts of data. The size of the tag can be based on its application environment (e.g., rugged, harsh). RF/ID systems can be linked to a satellite to collect data anywhere in the world from a home-base station. RF tags are more secure than bar codes, they can have memory partitions that are password protected, they are very difficult to counterfeit, and the systems are extremely accurate, with calculated error rates as low as 1 in 100 trillion. [TUTT94, pp. 361, 365]

RF/ID technology can be used in many applications. The tag can be made in numerous shapes, sizes, and configurations, can be passive or interactive, and can operate in various frequency ranges. It can be used in centralized database operation or in decentralized database operations. RF/ID systems can provide accurate, timely information by allowing the host computer to interactively check data through the various terminals. RF/ID systems increase labor and equipment productivity, inventory accuracy, and customer service response time. They eliminate paperwork and reduce space and time requirements associated with various operations. RF/ID systems can provide a sound solution to the environmental challenges that other systems have failed to achieve. [DAVI91, pp. 28-30]

4. Weakness

One of the main weakness of all RF/ID technology systems (whether it is high, medium or low frequency) is interference created by metal objects that come between the reader and the electronic tag. Cardboard boxes are disruptive in these systems. Therefore,

proper tuning and tag placement can overcome these interference problems. [REBO94] Other weaknesses include the cost of the tags and the total RF/ID system. RF/ID tags cost about 100 to 1000 times more than a magnetic stripe card or a bar code applied to a card. RF/ID systems use more advanced technologies for their operation, the equipment can be large in size and more complex to operate, the hardware and software requirements are more sophisticated, they have higher procurement costs, which drives up the total system costs. Some RF/ID systems must adhere to FCC licensing regulation. [TUTT94, p. 361] Based on the media used for the RF/ID tag, it can be sensitive to extreme temperatures (e.g., burning) and some chemical solvents.

E.   OPTICAL CARD TECHNOLOGY

Optical memory cards were developed by Drexler Technology (California, USA) in 1981. [KAEB92] [DREX92] Optical memory card technology, also known as laser card technology, is based on optical recording technology.

1. Characteristics

Optical memory card technology involves the process of writing and reading with a semiconductor laser beam, a few microns in diameter, into a wide, reflective optical reading stripe encapsulated between transparent, protective layers of a card medium. The laser beam passes through the protective layering and forms tiny "pits", also known as "spots", along the tracks of the reflective layer. The presence or absence of pits on the card represent "1s" or "0s" of the binary code, which can be translated into numbers, characters, or graphics from the recording stripe. The pits on the optical card are microscopic in size, and can be as small as 2.25 microns. To retrieve information, the same semiconductor laser beam (set at a lower power intensity in the optical card reader/writer) scans the card, a photo sensor detects the reflectivity difference created by the pit sequence, and translates the readings into alphanumeric or graphic information for transmission to a computer system. Data can be read, new data can be written, and data can be deleted from user view at any time, but the deleted data can not be erased from the card. [CANON] The deleted

data remains permanently stored on the card, which later can be used as an audit trail to track all data changes to the card. [DREX92]

The optical card is typically the size of a standard credit card and has the digital data storage capacity of up to 2,400 pages of text or over 200 pages of document image files. Presently, the optical memory card data capacity ranges from 2.8 megabytes (MB) up to 6.6MB. [OMDT93] Optical memory cards are available with or without error detection and correction (EDAC). Optical cards with EDAC typically have less user data storage capacity due to the overhead of the EDAC features. [DREX92] The standard optical memory cards (2.8MB with EDAC to 4.1MB without EDAC) cost between $5.00 to $8.00. [INFO94, p. 24] Figure 2.6 is an example of an optical (laser) memory card.

Optical memory card technology is classified as write once, read many (WORM) technology. The card can be written to once in a specific area, and read many times from that area. When new data is enter on the card, it is written to a new area, and the previous existing data can not be deleted. Therefore, all the changes to the data on the card can be tracked which provides for the audit trail capability of this card technology. [INFO94, p. 15] In addition to the audit trail capability of this card technology, additional security features can be added to enhance data security. Security can be accomplished through
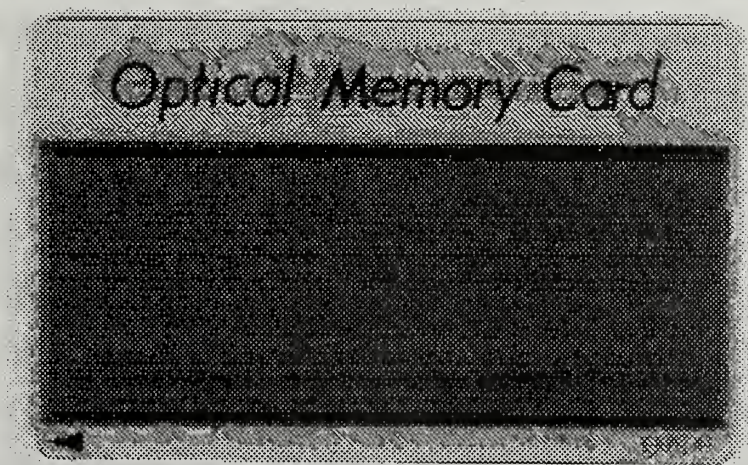
Figure 2.6: Example of Optical (Laser) Memory Technology

digitizing and storing personal identification numbers (PINs), photographs, signatures, voice prints, fingerprints, hand geometry, or extensive biographic data. [INFO94, p. 15] In use, the system can use the card information to validate and verify the person using the card is the authorized card holder. Data encryption programs can be used to protect the data from unauthorized use.

Optical card media is considered highly secure and durable due to its nonvolatile and environmentally tolerant memory. Since the card is physically etched by the laser light source, it is impervious to magnetic or electrostatic fields (electromagnetic interference - EMI). The card media with the transparent protective layers can withstand various temperature extremes ($-40°$ to $212°$ F) [CAPA94, p. 299], various chemical solvents, dirt, dusty environments, and severe impact. [INFO94, p. 15] The card can tolerates a high degree of flexibility without damage.

International Organization for Standardization (ISO) and International Electrotechnical Committee (IEC) standards exist for the optical card technology. ISO/IEC 11693 defines the general characteristics of the optical card, which consists of the optical card materials, construction, dimensions, and test environments. ISO 11694 defines the linear recording method, which includes the physical characteristics, the dimensions and locations, the optical properties, and the logical data structures. In particular, ISO 11694 Part 3 define the optical card recording area requirements of media reflectivity, data signal quality, and optical layer characteristics. The optical card meets the ISO 7810 standard for overall size and shape. [CALL94]

The optical memory card system can be used on-line or off-line and has interface capabilities with other equipment. When the card is used on-line, it can be associated with a centralized database for reading and writing information. When the card is used off-line, it can be associated with other technologies, such as radio frequency identification, to support functions for decentralized database applications. The optical memory card can store a variety of information, basically any form of information that can be digitized, e.g., text, document images, graphics, sound, voice, video, biometrics, photographs, x-rays, and fax transmissions. Therefore, it has interface capabilities to support its use with various

equipment, to include scanners for fingerprint, hand scans, and X-ray; full page scanner; digital scanner; and signature pad. In addition, the reverse of the card is available for other uses, such as photographs, bar codes, fingerprints, logos, and the prints can be in color or in black and white. [INFO94, p. 15] [OMDT93]

2. Applications

Optical memory card technology has been used in many applications. It is an ideal storage medium for health/medical card systems, publishing systems, record keeping systems, identification card systems, promotional systems, [INFO94] consumer transaction systems, and document storage [DREX92]. It has been successfully used in health care systems as a health care card, an electronic medical record to store emergency medical information, health plan record, next of kin record, immunization history, radiology history, bilateral mammography radiograph (baseline), prescription history, DNA footprint, and as a general medical history record; in patient tracking (including the information from above) for patient arrival, processing, departure, and daily processing/ billing; in travel history tracking for passport/visa/work permit imaging and immigration security and control; in student identification/education record history systems for academic records, special education program history, and medical/immunization records [SPAR94]; library card system [SPEC93]; and in military operations for logistics applications. [CAPA94, p. 294]

3. Strength

The main strengths of optical card technology is the high data storage capability of 6.6MB, it can be used with or without EDAC, its has valuable security and audit trail capabilities, it is extremely durable and environmentally tolerant of external conditions, and it is resistance to EMI. Other strengths include: the existence of established standards for this card technology, it can be used to store a variety of digitized information; the card system can be used on-line and/or off-line, so it can support passive and interactive operations with centralized and decentralized databases; it has various interface capabilities with other equipment to include scanners for fingerprint, hand geometry, X-ray, full page

scanner, digital scanner, and signature pad; it can support various applications; and it can complement other technologies, such as RF/ID systems. In addition, the reverse of the card is available for other uses, such as photographs, bar codes, fingerprints, logos, and the prints can be in color or in black and white. Cost per byte of data storage capability is low compared to other card technologies (e.g., $5.00 to $8.00 for 2.8MB to 4.1MB of data storage capacity). [INFO94, pp. 15, 24]

4. Weakness

The main weakness of this card technology compared to bar code and magnetic stripe card technologies is the cost of the card, in general, ($5.00 to $8.00 for optical card compared to $.10-$.25 to $.85-$1.50 for bar code or magnetic stripe, respectively) [INFO94, p. 24] and the associated cost encountered from the increased complexity of the hardware and software of optical card based systems. Being a relatively new technology, this technology presently does not have the supporting infrastructure for its use, compared to bar code and magnetic stripe technologies. Optical card systems require human contact for the card to interface with the reader system. In addition, the optical card systems are not very portable and the reader/writer component is sensitive to movement. [ZAGU94] [DEPT94, p. 3]

F. INTEGRATED CIRCUIT (IC) CARD TECHNOLOGY

The smart card, super smart card, and PCMCIA card are IC card technologies. [SEID94, p. 207] Each of these IC card technologies have different physical and operational features, different functional capabilities and areas of applications. The following sections defined and identify these card technologies and their applications to facilitate a better understanding of their functional capabilities.

1. Smart Card Technology

Smart card history began in the early 1970s in Japan and in France. In 1970, Kunitakda Arimura invented a plastic card incorporating one or more integrated circuit chips (ICC). [WON91, p. 4] He filed the first patents in Japan, in March 1970. [TOWN93]

But, due to the smart card development in 1974, by a French journalist, Roland Moreno, who had world-wide patents for inventing a card with a self-protected, integrated memory, France was given credit for the development of smart card technology. [TOWN93] In 1974, Kunitakda Arimura invented the contactless card. [WON91, p. 4] In retrospect, smart card technology has been around for 20 years.

Some people have wondered why has it taken so long for this technology to mature if it has been around for 20 years. Various reasons have been given to include the United States placed more emphasis in magnetic stripe and other card technologies during the 1970s, and smart card critics in the United States noted that smart card technology was better suited to France in the 1970s. France, historically, had high telecommunication costs and a poor infrastructure for authorizing card transactions. Developing a technology and a system to use this technology was desperately needed and France was willing to make this commitment and investment. [KUTF93]

a. Characteristics

The "smart" or "integrated circuit (IC)" card is an automatic data collection and identification card technology that uses a credit-card size plastic card with one or more embedded integrated circuit chip or microprocessor chip. Many names are given to classify and categorize this smart card to include Memory Card, Chip Card, Integrated Circuit Card, and IC Card. The smart card is best known because of its built-in logic ability. [TOWT93] The control logic and the memory are located on the same chip. Smart card memory can be either electrically programmable read-only memory (EPROM) or electrically erasable programmable read-only memory (EEPROM). The chip, made of silicon, is placed between two layers of plastic. [LAT92] Figure 2.7 is an example of a smart card with an integrated chip.

Various types of smart cards exist. The smart cards can be contact, contactless, wired logic, EPROM, EEPROM, microprocessor-based and Super Smart cards. [TOWT93] The microprocessor card has a microprocessor chip with a chip operating system (COS) or multiple-application chip operating system (MCOS). The microprocessor
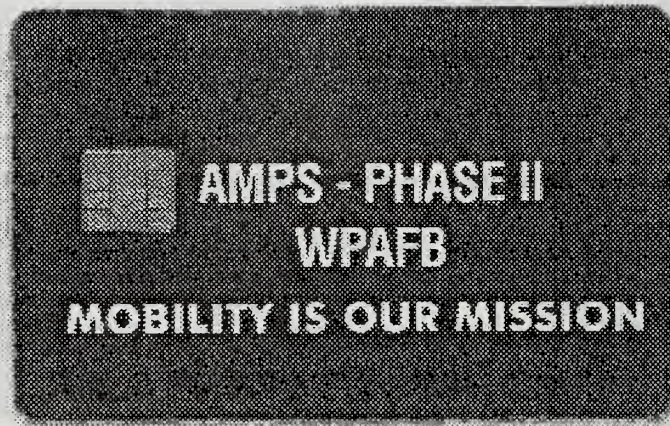
Figure 2.7: Example of Smart (Integrated Chip) Card Technology

chip has the capability to be programmed, to manage memory, and to process and store large amounts of electronic data. The smart card with this type of chip is considered to be alterable. The alterable smart card allows information to be added, with the previous existing information protected so it can not be erased. The term "smart card" is also applied to a plastic card that only contains memory chips known as a "serial memory" smart card, "IC ROM" card, or "IC memory" cards. IC ROM cards are considered to be the unalterable version of smart cards, they have no programmability, [DAVI91, p. 32] and can store up to 16 KB of information. [KRUE94] This memory smart card contains flexible rewritable serial memory (EPROM or EEPROM) for data storage. [DATACARD] IC cards that do not have processors are similar in function to optical memory cards. [DAVI91, p. 32]

The smart card is activated by an external electrical power source, such as a card reader or data terminal, to the integrated circuit chip by contact or contactless technologies. The small chip can hold a tiny semiconductor and electromagnetic memory. The interfacing device interacts electronically with the chip on the card to provide the chip's power with the correct voltages, frequencies, and current characteristics. The signal

interface provides the logic and data information flow (e.g., the intelligence and electromagnetic memory) to perform applications. The logic of the chip is a key feature of the smart card which yields its intelligence capability to provide and follow instructions, make logical decisions, respond to external commands, and provide the requested information. [SVIG87, pp. 1, 39] The memory features of the chip give the smart card the capability to act as a small portable database. [VANC90] These features are key for smart card use in decentralized database applications and use as an authentication device.

The smart card can have various memory capacity for storing data with different associated costs. The data storage capacity can vary from less than 1K up to 64K. [INFO94, p. 24] Based on the type of smart card and the data storage capacity, the smart card can cost between $1.45 and $26.10 per card. [SEID94, p. 208] Research is constantly being conducted to achieve increasing storage capacity of this card medium.

The technical challenge in the development of the smart card is designing the card package to hold the chip for various applications. The packaging design will need to address the thinness and flexibility of the card, and how the chip on the card will interact with the read/write devices. The chip is produced on a relatively thick silicon base that can be very rigid and may be brittle. The smart card can be designed with contact or contactless interface chip features. The contact smart card has its contact points open to the environment for it to have point-to-point contact with the reader/writer device. The conductive leads of the chip's circuits must contact the interfacing leads of the reader/writer device for any read/write interaction (information exchange) to take place. The leads of the chip need to be flexible to survive bending, twisting, and/or torsion forces applied to the card. The contactless smart card does not have its integrated circuit chip open to the environment and does not require point-to-point contact with the reader/writer device. The contactless smart card can be made in two ways, by the use of inductive coils or by small, high-frequency transmitting and receiving antennas that power the smart card through the signaling process. Both smart card designs must address impact forces that occur from the use of embossing or imprinting equipment. [SVIG87, pp. 40, 44]

The smart card has security capabilities. The chip memory can be divided into logical channels zones with each zone having a different security level to meet the required information sensitivity level of the data. [MADA, p. 49] Microprocessor cards offer secure information processing and management through data protection and encryption methods. The Data Encryption Standard (DES) or other algorithms can be used to support security of information on the card. [BRIG92] In operation, the microprocessor stores the passwords and codes which trigger the software sequences on the computer system for authentication and authorization of the card user. [STON87] The serial memory smart card offer read and write memory protection and can be used with a personal identification number (PIN) for added security. [BRIG92]

ISO standards have been developed and implemented for smart card technology. The smart card meets ISO 7810, the physical characteristic standard for credit-card-size cards. The ISO standard for the integrated circuit card is ISO 7816. This standard has various parts to discuss the various characteristics of the cards: Part 1 describes the physical characteristics, Part 2 describes the dimension and location of the contacts, Part 3 describes the electronic signals and transmission protocol, Part 4 describes the inter-industry commands and responses, and Part 5 describes the registration system for application in IC cards. ISO 7813 describes the identification card requirement for financial transaction cards, DIS 9992 describes the message criteria between the integrated circuit card and the card acceptor device for financial transaction cards, and DIS 10202 describes the security architecture of financial transaction systems using integrated circuit cards as financial transaction cards. [GEMPLUS]

Smart card use is expected to be a key element in the truly cashless society, which may change the shape of the world in financial and non-financial transactions. Over the years, the increased use of the smart card had been held back by the high costs of the cards, the heavy investment in magnetic stripe technology, the resistance to change, and the lack of development tools and standard software. [SCHN91] In 1982, the smart card cost $18 and the support system cost were very expensive. [HOWA82] It has been noted that

while smart cards are more costly, the economies of scale will affect its uses; as their use increases, the card's cost will decrease. [THOG83] Since the 1980s, the card costs have been coming down to about $5 to $10 per card and the support system issues are being addressed with various innovative card reader/writer devices. In general, the smart card still costs about 10 times as much as a magnetic stripe card. The reality is smart card use will evolve when manufacturing and marketing of the card is economically feasible. [MADA92, p. 51]

One powerful incentive for using smart cards is the escalating cost of fraud connected with the magnetic stripe cards, whereas the smart card has valuable security capabilities. The magnetic stripe card has simplistic attributes that function with adequate security within a limited operational environment. However, the smart card, with its silicon chip, can do everything that a magnetic stripe card can do, and more. [SCHN91] The intelligence, programmability, increase in memory capacity for information storage, processing of information on-call and advances in integrated circuit technology will permit multi-application use of the card, with each application having its own security keys and access rules. These smart card features offer value-added functionality when compared to the current magnetic stripe card and bar code systems. [MADA92, pp. 50-51]

b. Applications

Just as personal computers strongly influenced the 1980s, the smart card will effect every industry and profession in the 1990s. In 1992, the average smart card had the computing power of an IBM PC of about 5 years ago, but with less memory capabilities. A key event for promoting smart card use is marketers' involvement. Three new opportunities exist to influence the use of smart cards, which include a whole range of new products and services, significantly improved customer service, and more sophisticated database marketing. New ideas and application areas for smart card use are evolving every day. The main hurdles that must be addressed to fully implement this technology are the cost (hardware, software, and card costs) associated with the technology, an identified and

implemented infrastructure, and educating the world to the many features and uses of this technology. [MITC92]

Since the smart card's inception, it has been used in various applications. In 1982, more than 150,000 smart cards were being used in France, primarily by banks and retail outlets. In the United States, the card was being used in experiments involving banking transaction, at-home shipping, electronic mail, and other videotex services. Various United States government agencies showed interest in the card to combat fraud and duplication and envisioned the card could be viable in storing personal medical data. During that time, and even today, the concept still holds true, the card's use is only limited by one's imagination. [WHAL82]

Since the early 1980s, smart card technology has been maturing and its application areas have increased. One of it's main uses is as a portable carrier of data which can be updated with each transaction. A terminal can read and process the card information and can write information back to the card and to a centralized or decentralized data base. The card has the capability to operate passively or interactively with implemented smart card system. The chip on the card can hold the necessary data to manage several independent applications in finance, insurance, health care, travel, transportation, government, retailing, and security. The smart card has unique advantages in use as an identification and access pass, encryption device, personal record, carrier of electronic authorization and tickets, and electronic money. [MADA92, p. 49] The smart card has a wide range of communications and marketing applications, ranging from providing secure access to computers to unscrambling satellite television signals. [LAT92] Smart cards are well-suited for record-keeping and identification applications. [HEAD91]

In finance, potential smart card applications include credit-line authorization, financial history qualification evaluation, automatic bill-paying, off-line point-of-sale (POS) transactions, and use as a pre-payment card, e.g., cash card. In these areas, smart card use can lower the bank operational costs. [THOM83] Business can be completed at the transaction terminal for user verification, account balance checking,

purchase authorization, sales processing, and receipt generation. [KUTL93] In addition, memory cards can be used as bank ATM cards and will depend on the terminal for their intelligence. [HEAD91]

Various identification systems use smart card technology. As an identification device, the smart card can retain biometric images through human eye retina recognition, fingerprint recognition, hand geometry, signature dynamics recognition, and voice recognition. [WON91, p. 2] Smart card technology has been identified and tested for use as a carrier of information in military applications, and as a portable personnel data carrier with the Soldier Readiness Card (SRC), Multi-Technology Automated Reader Card (MARC) programs, [MARC94] and the Automated Mobility Processing System (AMPS). [REBO94]

Smart cards are used all over the world. Examples include: in France, smart card technology is used in telephone and television payment systems; in Italy, motorists use smart cards to pay tolls and they are used for pay telephone systems; in Spain, season ticket holders use smart cards and a fingerprint as their admission ticket; and in the United States, smart cards are being used as security access devices. [FLOO92] As a reflection of the world's smart card use, smart card sales in the European market are expected to grow from 114 million in 1992 to 235 million by 1995. In contrast, the United States' market uses about 1 million smart cards. Smart card use is expected to increase as more large companies become involved in the marketing efforts. [LAT92]

The United States still has a limited number of smart card-based systems. The United States bankers are still fighting the cost justification hurdle of smart cards relative to conventional, cheaper magnetic stripe cards. They are concerned with privacy of the data as smart card use increases in the United States and in the world. Despite these concerns, some United States banks are exploring prepayment and smart card use. [FLOO92]

In summary, the smart card has great application potential with its power, speed and processing capability of a modern computer, security of electronic data, and it can be packaged in a convenient form to be carried by a person. [WON91, p. 1]

c. Strength

The major strengths of smart card technology are its security capability, its logic (intelligence) capabilities, its interactive (read/write) capabilities, its memory storage capability, it programmability, its flexibility for multiple application utilization on one card, and established standards for its implementation and use. Other strengths include its data storage capacity, its application for centralized or decentralized database use, its integration with other technologies on the same card ("Hybrid" card), and the use of the remaining space on the card for other purposes, e.g., advertising, logos, identification information. [BAND91] [INFO94, p. 16]

The security features of the smart card technology result in highly secure systems. With the capability to store biometric information and the data encryption capabilities, this card technology can be used as a positive identification and authentication mechanism. These features provide for improved access control management; privacy for confidential data; resistant to duplication, counterfeiting and tampering; and audit trail capability to track card use. Smart cards can not be duplicated or copied without the correct hardware and software (including encryption software) and they have the capability of locking themselves when fraud is detected. [MILM84]

The smart card may have temporary or permanent data storage capability and may contain a self-programming one-chip microprocessor which provides for its interactive features. The programmability and interactive (read/write, active/passive) capability of the smart card promote its use in centralized or decentralized database applications. The card can be used to promote "off-line" verification and approval of transactions. [KUTL93] Being programmable, the smart card can be changed to adapt to the changing environment when the need arises. With its logic and intelligence capability,

the smart card can provide and follow instructions, make logic choices, and follow alternative decision paths.

With the smart card's interaction with the card reader/writer, the transaction can be stored directly on the card and the information does not need to be immediately transmitted over a network and/or the telephone lines. The smart card has easier connection, direct electronic readability, and better control functionality compared to other technologies. [SVIG87, pp. 172-173] In addition, the smart card can eliminate paperwork when used at a POS terminal, and can reduce customer and company personnel mistakes. Therefore, the benefits enjoyed by companies and service providers that use smart card technology include secure, timely, and accurate data processing that leads to efficient operations and reduced operational costs. [BRIG92]

Smart card technology can be used to automate many applications. The smart card can be used for a tailored application or for multiple applications. Smart card technology is considered as having "Hybrid Technology Integration Potential" or the capability to have other card technologies on the same card. [INFO94, p. 16] In addition, smart card technology can support prepayment operations, where the card is assigned a cash value and decremented with each purchase transaction. In general, smart cards have all the advantages of credit cards with magnetic stripe technologies, without the drawbacks. [MILM84] Applications requiring intelligence, data storage, flexibility, and security lend themselves to smart card use.

d. Weakness

The major weaknesses of smart card technology are the cost of the card technology (including the supporting hardware and software systems), the lack of a supporting infrastructure, the concern for protection of privacy information, packaging of the chip on the plastic card (contact or contactless), and environmental conditions affecting the card use.

The lack of a revolution to adopt smart card technology has been a topic of discussion for many years. In 1983, it was projected that even with improvements in the smart card, the concept was not expected to be immediately and fully embraced by United States financial institutions due to investment in other card technologies (e.g., magnetic stripe technology). Other reasons for its slow implementation and use in the United States included the high cost of smart card technology and the reasonable cost of the paper-based transaction system. [THOT83] The environmental conditions that affect card use include temperature extremes, contact with chemical solvents, improper handling of the smart card, to include use as an ice/snow remover and leaving the card in areas of heat or direct sunlight. In addition, the contactless and contact smart cards are susceptible to damage from bending and improper manipulation of the card.

e. Contact Versus Contactless Smart Card Technologies

In their own way, contact and contactless smart card technologies have their own strengths and weaknesses which must be addressed. The strength of the contact smart card compared to the contactless smart card is the reduced cost associated with the card system. Overall, though, the contactless smart card features definitely outweigh the contact smart card. The contact smart card has its contact points open to the environment for it to have point-to-point contact with the reader/writer device. The contactless smart card does not have its contact points open to the environment which increases the durability of the card. The associated environmental and durability factors of the two types of smart cards are key criteria for their application in various environments. The contactless smart card is highly durable and has some resistant to static electricity, chemicals, and water (moisture, relative humidity). The contact smart card is not as durable as the contactless smart card, and it is susceptible to static electricity, chemicals, dust/dirt, and water when these substances come in contact with the exposed contact points. Chemicals can be corrosive to the contact points of the contact smart card, can affect the protective covering on the contact and contactless smart card, which can ultimately affect the integrated chip. Contactless

44

smart card systems have fewer mechanical parts, resulting in increased serviceability and reliability. This leads to lower operational and maintenance costs which may results in a better return on investment. [BAND91]

2. Super Smart Card Technology

The Super Smart Card is an integrated chip technology that has an integrated display and a keyboard. [SEID93, p. 21] It has a built-in battery to supply power to the card. It is basically four cards in one. It is a metallic card with raised embossing. It has magnetic stripe operating characteristics without the stripe. It has a stripe simulator that emits magnetic fields. However, the simulated stripe can not be used in an ATM-like card system which require the stripe to be moved through the read/write heads. It is a smart card with logic capabilities. And it has a crystal display of various characters, numeric pad, function keys, [SVIG87, p. 91] clock, calculator, currency conversion, and a notepad. It can be used for credit, debit, prepaid, and security applications. [SEID93, p. 21]

3. PCMCIA Card Technology

The PCMCIA card technology came about in the late 1980s. The PCMCIA card technology was created as an open architecture unit with self-contained bus-architecture components that would interface with computers, especially notebook systems. The PCMCIA components were first devised to be add-on memory cards for small computers to address the need for additional storage since a large hard disk drive was not feasible for use in a small computer system. [LEFK94] Therefore, the mission of the Personal Computer Memory Card International Association was to establish a standard for making and marketing these credit-card size "memory" devices. [RIST93, p. 264] Various other names used for or in association with PCMCIA cards are PC Cards [RIST93, p. 264], IC Memory Cards [SEID94, p. 207], and Magnetic Memory Cards [INFO94, p. 17].

a. Characteristics

PCMCIA specifications rapidly developed in the 1990s. In 1990, the PCMCIA Specification Release 1.0 was adopted, which designated the standards for incorporating various "memory" technologies onto Type I PCMCIA cards. In September 1991, Release 2.0 revised the PCMCIA specification to include standards for "input/output" (I/O) cards, known as Type II cards, for products such as modems, LAN cards, network adapters, mass storage, and other peripherals. Not long after Release 2.0 was Release 2.1, which included support for a larger size Type III PCMCIA card used mainly for miniature hard disks. Recently, Toshiba, a leader in this technology, designed a 16mm slot to facilitate modem makers building RJ-11 plugs for notebook computers. The PCMCIA modem card is to be used in a slot instead of attaching the modem to the system through the communication ports. [RIST93, pp. 264, 266] At the present time, the PCMCIA Association recognizes the standardization of Type I, Type II, and Type III PCMCIA cards for various uses. The Type IV PCMCIA card has not been recognized as a standard and its development and use remain proprietary. [CHAN94] The noted sizes of the Type IV card are from 15mm to 18mm. [HADE94] Figure 2.8 is an example of a PCMCIA card.

The four types of PCMCIA credit-card sized devices differ based on their thickness and use, which includes the allowance for built-in devices drivers. Table 3 identifies the different card types, thickness features, use and pin connection considerations. [LEFK94] [RIST93, p. 266]

PCMCIA specifications were established to be backward-compatible. Under these specifications, as an example, Type III cards can be used where Type II cards can be used. Building one level of the specification upon the other ensures that the cards will be forward-compatible as well as backwards compatible. In addition, PCMCIA systems are "2.1-compliant" if their sockets can accept two Type II or one Type III card (at least 10mm high), and if the controller chips of the system can address the interrupts and memory areas used by Type II and Type III cards and their drivers. [MILB94]

46
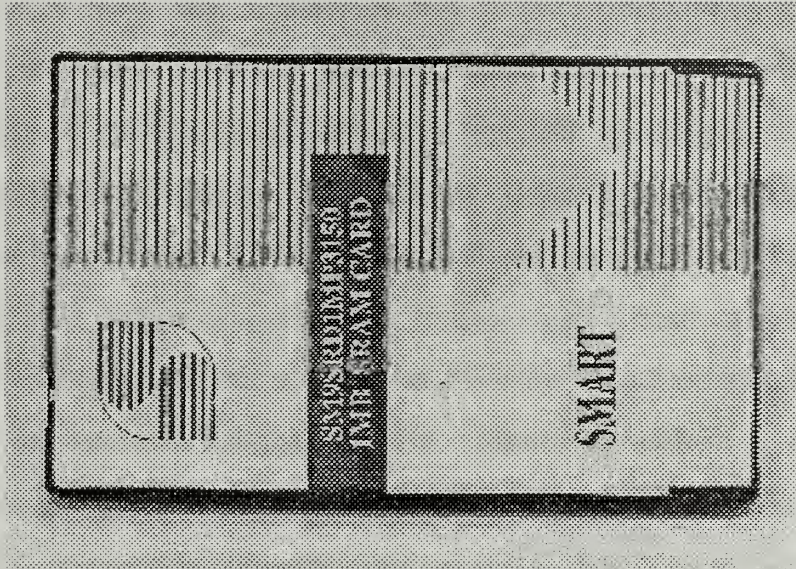
Figure 2.8: Example of PCMCIA Card Technology

TYPE	THICKNESS	USE	PIN CONNECTION
Type I	3.3 mm	Memory	68-pin connector 2 parallel 34-pin sets
Type II	5 mm	Input/Output (I/O) Fax Modems LAN adapter cards Slim Media (Communications)	68-pin connector 2 parallel 34-pin sets
Type III	10.5 mm	Miniature hard drive (used for rotating disk drives)	68-pin connector 2 parallel 34-pin sets
Type IV	15-18 mm	Large hard drives	Proprietary (Toshiba)

Table 3. PCMCIA Card Characteristic. [LEFK94] [RIST93, p. 266]

A working PCMCIA system has several layers, which includes hardware to software requirements. At the lowest level is the host adapter, which is an interface chip that connects the computer's expansion bus to one or more (usually two) 68-pin PCMCIA sockets. The most commonly used adapter is the Intel 82365SL chip.[3] The host adapter is configured to respond to specific memory and I/O ranges to satisfy the PCMCIA card requirements. It handles the interrupts generated from the PCMCIA card and provides some power-management functions. The software requirements are designed in the Card and Socket Services, which are specified in the PCMCIA driver. The Socket Services are the lowest layer of the PCMCIA system software architecture. The Socket Services' primary function is to relay communication between Card Services and the host adapter. Socket Services is hardware dependent and configures the host adapter to operate properly with the PCMCIA card and their associated drivers. Card Services is a higher software layer that manages the PCMCIA card resources throughout the system. The Card Services' function is often performed by a higher-level Card Services client driver. PCMCIA card characteristics of compatibility, interchangeability, and the ability to insert and remove cards without the need to reboot the host system ("hot swapping") are dependent on the Card and Socket Services software. [STAM93, p. 268]

Card and Socket Services drivers are essential to the installation of the PCMCIA card to operate on any PCMCIA-capable system. For installation and operation of any PCMCIA card, the hard disk requires the Socket and Card Services drivers be loaded into the BIOS, the CMOS configuration or into memory through the system's CONFIG.SYS file. The system BIOS must be set up to access the PCMCIA card and the PCMCIA controller chip must be recognized to run any PCMCIA device. In general, the Card and Socket Services drivers alert the system to the presence of PCMCIA slots and

---

[3] As of December, 1993, the Intel chip was the industry standard for PCMCIA controllers. [RIST93, p. 267]

allow the host system to interpret and interact with the PCMCIA device. The hardware circuitry must match the signals of the PCMCIA cards to the host system for correct system operation. [LEFK94]

Four categories of PCMCIA card drivers exist above the Card and Socket Services. These categories are generic device drivers, Card Services client drivers, super client drivers, and enablers. Some drivers specifically use Card and Socket Services and other drivers bypass these services. Generic device drivers initialize PCMCIA cards that perform well-defined functions, such as Static Random Access Memory (SRAM) or certain hard disk cards. Hard disk cards with standardized interfaces will operate in most PCMCIA systems that have Card and Socket Services installed. Card Services client drivers typically are card-specific drivers that use Card and Socket Services and perform card initialization and resource management functions. Super client drivers, using Card Services features, are capable of recognizing and configuring various PCMCIA cards. Enablers are typically card-specific drivers that bypass Card and Socket Services and communicate directly with the host adapter. Enablers are the most popular kind of driver to use, especially for products like modems and some solid-state storage devices. Enablers do not allow "hot swapping" of PCMCIA cards. [STAM93, p. 269]

The minimum set of software and hardware requirements for PCMCIA card technology is defined in the Exchangeable Card Architecture (ExCA) specification, initially defined by Intel. As a rule of thumb, if a card requires a system reboot to activate it, then it is not Card and Socket Services compliant. [STAM93, p. 268]

There are two types of "memory" chips used for PCMCIA cards, the SRAM chip and the flash memory chip technology. A PCMCIA card with a SRAM chip is typically used as a small mass-storage device with data storage capacity from 1MB to 2MB and requires on-board batteries to provide a constant power source to retain the data. A PCMCIA card with a flash memory chip has data storage capacity from 1MB to 40MB, uses Electronically Erasable Programmable Read Only Memory (EEPROM), and requires

no on-board power source. Flash memory can be erased all at once, "in a flash" as its name implies. [LEFK94]

Flash and SRAM chip technology have different operating characteristics which address different application areas. A flash memory card requires no configuration drivers, it does not require a lithium battery inside the card, it has lower power consumption, higher storage capacity, and lower cost when compared to a SRAM PCMCIA card. Without the need for configuration driver, the flash memory card is a simple peripheral to install and use if it is compatible with the host system. If the flash memory card is not compatible with the system, it can be difficult to use. Flash memory voltage requirements meet the 3.3 or 5 volts needed for write and erase operations in the small computer systems. PCMCIA cards with flash memory have storage size in the 40MB range, and can be expanded up to 80MB with preloaded data-compression software. [RIST93, pp. 263, 269-270] Therefore, PCMCIA cards are available with various data storage capability (1M up to 64MB) and application features. Prices range from $44 [AITC94] to over $1000, and depend on the PCMCIA card-type and application features. [HADD93, p. 389] One drawback to flash memory is when one file needs to be changed, the whole card must be written over again. In comparison, SRAM PCMCIA cards operated like a floppy disk, but with a battery. SRAM PCMCIA cards can be read or written to, files can be changed and rewritten to the card without the requirement to rewrite the whole card. [ZAGU94]

Two issues that must be addressed with flash memory are formatting and writing to the flash memory card and chip incompatibilities. Flash memory cards typically use the DOS format command to format the card and it is ready for use. Some systems do require proprietary formatting. In use, a flash memory card is slightly slower than a SRAM card due to the different way it writes data. Some cards do not perform contiguous writes, but run algorithms in the background which search for open spaces and writes to them as needed. [LEFK94] For compatibility, the system's host-adapter chip set and the flash memory card chip should be able to communicate. Chip incompatibilities can occur if the

flash memory card chip's EEPROM is programmed for a particular PCMCIA host-adapter chip set. [RIST93, p. 267]

PCMCIA architecture incorporates four key features into the PCMCIA card development. The four features are host independence, easy installation and configuration (also known as "plug and play"), hot swapping and execution in place (XIP). Host independence provides for the capability of the PCMCIA card to run with any computer carrying a PCMCIA-compliant interface. This concept supports the possibility for the same PCMCIA card being ran on various personal computers with a compatible PCMCIA socket. Easy installation and configuration is based on the concept of "just pop a PCMCIA card into the slot, turn on the system and the card automatically configures itself," preparing the system for use, hence the term "plug and play." Hot swapping refers to the ability to pull one PCMCIA card out of the system, insert another, and keep on computing without rebooting. The execution in place (XIP) feature allows software loaded in ROM on a PCMCIA card to run without being loaded into the host system's RAM. This feature is useful to have with systems limited in their amount of internal memory and the lack of internal floppy drives, like subnotebooks and palmtops. [RIST93, p. 264]

Compatibility issues that have affected other card technology system have hampered the "plug and play" and the "hot swapping" features of the PCMCIA card systems. At the present time, the system must know, via the hardware and the software, if the port the PCMCIA card wants to use is already being used. This hardware to software port checking restricts the "plug and play" and the "hot swapping" feature of the PCMCIA card technology. [RIST93, p. 265]

b. Applications

The PCMCIA Card market has continually expanded to accommodate various technologies, increasing the interoperability and the flexibility of this technology to support various application areas. [SHAF94] The peripherals made with the variety of PCMCIA cards include memory (SRAM and flash memory), mass storage, local area

network (LAN) adapter cards, portable fax/modem cards, wireless communication devices [LEFK94], pagers [SHAF94], sound cards [ZIFF94], portable telephones, personal health-care data carriers, and video entertainment. [RIST93, p. 273]

The increasing trend towards mobile computing, the increasing sales of notebooks, laptops and palmtops, and the increasing storage needs of these systems have created an increased demand for various PCMCIA card add-ons. In 1993, the communication area had introduced approximately 30 different fax and data modem cards [SHAF94] with various data transfer rates, e.g., 2,400 bps, 9,600 bps and 14,400 bps. [RIST93, pp. 266, 269] The modem cards can use V.42bis and MNP5 data compression methods and they can have a built in automatic feature negotiation function. [OMAL94] Many notebooks are being manufactured with a PCMCIA slot vice having an internal modem. For modem compatibility, the modem cards use card enabler programs. The critical issue is how the enablers interact with the system's (e.g., notebook) PCMCIA controller. [RIST93, pp. 266, 269] [LEFK94] PCMCIA peripherals can be used for software distribution as well as data interchange. [LONG94] The technology is being held back for this application due to its prohibitive memory media cost and the licensing agreements from software companies. [RIST93, p. 273] For storage device application, research is being conducted on a new form of layered media that will allow up to 400MB in a Type I size card. New cards will include sound and solid-state storage. [RIST93, p. 273] PCMCIA card technology is projected to be a replacement for floppy disks and drives.

PCMCIA Type II and Type III cards are being used as PCMCIA network adapters. PCMCIA network interface cards (NIC) pose a different set of problems because of the designs of individual systems. They typically require Socket and Card Services drivers to be loaded through line statements in the CONFIG.SYS file. In addition, some NIC compatibility issues will develop from systems with a proprietary design and these systems must rely on proprietary cards. Since all NIC cards require some degree of proprietary driver loading, the factors that will distinguish one card from another will be price and ease of use. [LEFK94]

PCMCIA card technology has its place in portable and desktop computing and the notebook and personal digital assistant (PDA) markets. The technology is improving to the point where hundreds of PCMCIA peripherals are available. [ZIFF94] Cost and compatibility concerns will be factors in the future purchase and use of these products. [LONG94] As the trend for the use of PCMCIA technology increases, and numerous companies specialize in developing products based on this technology, economies of scale will be reached. [RIST93, pp. 274-275]

c. Strength

PCMCIA card technology has many strengths. The various PCMCIA card types are extremely flexible and adaptable, [LEFK94] which promote its use in various applications. It is used as a storage medium, with storage capabilities from 1MB to in excess of 80MB, and it has read/write capabilities, which promotes its use for active and passive operations. Based on its storage capacity, and its durable plastic casing, it is seen as the replacement for floppy disks and floppy disk drive systems. It can be used to store software programs to include security programs, leading to highly secure computing capabilities. The backwards compatibility feature and the Cards and Socket Services software and hardware features promote its use with other equipment (e.g., notebooks, laptops, palmtops, PDAs). [MILB94]

With various PCMCIA card technology standards, some compatibility and interoperability issues can be addressed, e.g., the choice to use standard drivers for maximum compatibility of system components. In addition to implementing standards, the future key advantages of PCMCIA architecture, host independence, easy installation and configuration, hot swapping and execution in place (XIP), are valuable features for PCMCIA card use. [RIST93, p. 264]

PCMCIA card technology has future capabilities for various applications. As the technology improves and economies of scale are achieved, the PCMCIA peripheral use and application areas will increase. PCMCIA will have a place in portable and desktop

computing applications. [ZIFF94] In addition, the cost per byte of data storage capacity for file storage and retrieval is low compared to other card technologies (e.g., $80 for 64MB of data storage capacity). [HADD93, p. 389]

d. Weakness

The main weaknesses of PCMCIA card technology are cost [ZIFF94], interoperability and compatibility concerns, lack of standards implementation, and it is more complex to use (e.g., Card and Socket services requirements with the host adapter). Other weaknesses include it is a new technology, therefore it is not a totally proven technology, and there is not an established infrastructure for its use. [LEFK94] Various vendors have interpreted the standards in their own way, which leads to incompatibility issues with the PCMCIA cards, the host adapters, and the drivers. The card incompatibilities limit its use and flexibility in the various card systems. [RIST93, p. 265] Various design concerns have affected card use, to include the physical size difference of the cards can affect their operation with a PC or small computer systems, the pigtail connectors of the PCMCIA peripherals can block adjacent card slot use, the 68-pin connector capacity might not be able to support the future 32-bit throughput and high data rate demands, and the various power demands can affect the card system operational capability. [ZIFF94] PCMCIA card is a magnetic media device and therefore it can be affected by EMI sources. The card has a plastic outer surface which can be affected by environmental conditions (e.g., excessive temperatures, burning, and chemicals).

G.   MAGNETIC INK AND OPTICAL CHARACTER RECOGNITION TECHNOLOGY

Magnetic ink character recognition (MICR) and optical character recognition (OCR) are not new automated identification technologies, since they have been around for many years. The applications of these technologies has mainly been with paper or printed materials and not for AIT card applications. MICR has been used extensively in banking and related functions to print information on checks. [PALM91, p. 5] OCR has been in

commercial use since the 1950s and was initially designed to read "stylized" fonts, such as OCR-A. The "stylized" fonts include a full alphanumeric character set with special characters to be scanned or read mechanically. [DAVI91, p. 24] These two technologies have their place in automatic identification systems, but they have not been key technologies that have found a place in AIT card technology applications. The characteristics of these technologies will be addressed with reference to their present use and to understand where these technologies, compared to other AIT card technologies, could be applied in card technology applications.

1. Characteristics of MICR

Magnetic ink technology is used in printing information on checks. Software programs have been developed for personal and business use to create and print checks with certain printers that use magnetic ink toner. The software does check layout, digitized logos, signature block, and the necessary MICR coding required for bank processing, and automatically prints the checks. [KAWA94] The software should meet the document and magnetic ink standards established by American National Standards Institute (ANSI) and the American Bankers Association for its use. [MALL93] The advantages to customizing and printing your own checks are checks can be easily corrected to avoid ordering new ones, banks and telephone number can be changed, and one check stock can serve several accounts. [KAWA94] Today, there are personal finance programs which lets you use virtually any laser printer to print checks that can be processed by banks' automatic check scanners. [LEWI94]

2. Characteristics of OCR

OCR technology is comprised of "stylized" fonts to include a full alphanumeric character set with special characters to be scanned or read mechanically. OCR technology requires printer and reader systems to read the stylized font and process the information for further use. Various printers and reader systems can be used for OCR technology. The three categories of OCR readers are page readers, transaction readers, and hand-held readers. The various reader capabilities influence the OCR application areas. Page readers scan text

pages, either from digitized document images stored in the computer system or directly from paper sources. Transaction readers scan a relatively short stream of data, like account numbers on payment coupons or statements. Typically, transaction readers provide higher accuracy than page or text readers and they can be mounted on mechanical transport systems. Hand held readers are used primarily to enter data when other methods are impractical or too expensive. Retailers use hand-held readers to enter item numbers for price look up, for inventory control at the point of sale, and to speed up the check-out process. Hand-held readers are effectively used in general data entry applications where a user can selectively scan information from forms or other documents. [DAVI91, p. 24]

In comparison to other related technologies, OCR recognition is usually slower than bar code recognition. With the use of check digits or other editing schemes, the reading accuracy of OCR recognition is comparable to bar coding. Without the use of check digits or other editing schemes, the accuracy of bar coding is better than OCR. Transaction readers associated with OCR technology can be programmed to calculate the check digit of a scan line, thereby reducing errors to fewer than one in three million characters. [DAVI91, p. 24]

OCR technology is best applied where human reliability is required, high character density is needed, when type-written or computer-printed material must be read, and where conversion to bar code technology is infeasible, impractical, or too expensive. OCR is frequently used for billing processes, check reconciliation, libraries, publishing, payment processing, at point of sales (POS) in retail, and other general data entry applications. [DAVI91, p. 24]

3. Strength and Weakness

MICR and OCR take on functionality characteristic similar to magnetic stripe and bar code technology, respectively. Therefore, the strength and weakness and the supporting functional capability matrix information for magnetic stripe and bar code technology are applicable for MICR and OCR technology.

H. ENHANCING TECHNOLOGIES

Biometric and voice data collection, and machine vision are considered enhancing technologies to the AIT card technologies. These technologies are considered enhancing technologies because they are not card media themselves, they are data digitized from some form to be used for their value-added features to the basic card media. Biometric data collection is mainly used for identification purposes and with its use, the card technology can have enhanced security for user authentication. Voice data collection can be used for identification purposes or to activate systems that operate on voice recognition patterns (e.g., voice verification). [DAVI91, pp. 14, 34] Machine vision uses mechanical systems to read other AIT resources, such as bar codes, and transmits this data to the integrating system to make further logic decisions for operational processes. [INTERMEC] The following sections identify and discuss these enhancing technologies.

1. Biometric and Voice Data Technology

a. Characteristics

Biometric identification (biometric ID) and voice recognition technology are based on the capability to digitally store some personal trait as a means of personnel identification to a computer system or on some storage media for user authorization or authentication. Personal characteristics can be based on two types of features: physical or behavioral. Physical features include retinal scan which digitizes the blood vessels image in the eye's retina, iris scan, facial recognition, fingerprints, thumbprint, hand geometry, and vein patterns which identify the blood vessel arrangements in the hand or wrist. Behavioral features include voice patterns, typing patterns, and signature patterns. [CART94, p. 405] The digitized pattern of the personal characteristic can be stored on various AIT card media or in a resident data base for identification or future use. Therefore, the biometric and voice recognition systems are interfaced with personal computers and the card technology systems for added security of the card data. This data is used to validate and verify the person using the card is the authorized card holder. These systems can be

user independent or menu driven. At the present time, there are not any standards established for the development and use of biometric and voice data recognition technologies. [INFO94, p. 20] Voice recognition systems are ideal where speed, accuracy and real-time data are critical to the business needs or when an operator's hands and/or eyes are occupied. Voice data collection can be combined with radio frequency systems to allow for mobility of the operator while verbally capturing data. [DAVI91, p. 34] Figure 2.9 is an example of biometric technology, the digital thumbprint on a standard credit-size card, which can be used for identification and/or authentication.

Voice data collection and recognition systems operate in various manners. Voice data technology converts words, phrases or sounds, spoken by a human into electrical signals, and then transforms these signals into a coding pattern or machine-readable form that can initiate some action. The data is captured at the source which provides for real-time data collection. Voice data technology systems can operate as a stand-alone system or can be integrated with other technologies, such as smart card and optical card for identification. Voice recognition systems can also be used to activate systems for other operations.
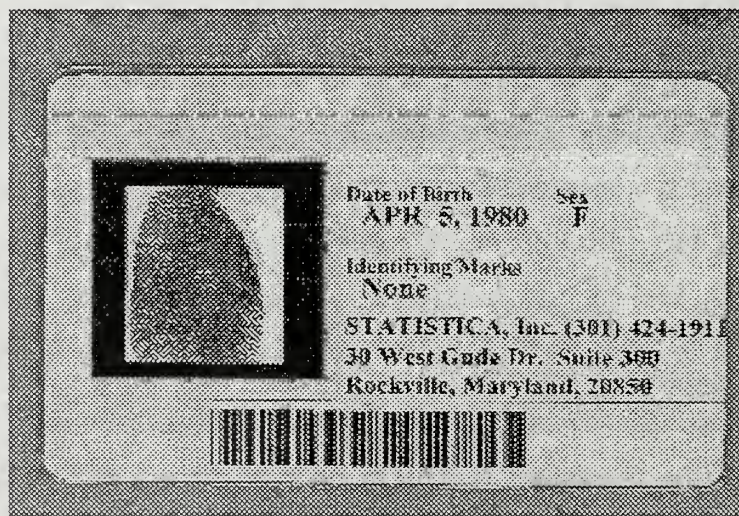
Figure 2.9: Example of Biometric Technology (Digital Thumbprint)

An operator can wear a microphone/speaker headset or use a telephone-like handset connected to a unit that identifies words and/or phrases in a programmed vocabulary and converts them into analog or digital electrical signals. The electrical signals are decoded by template matching or feature analysis. The decoded signal is transmitted to a personal computer or to a stand-alone voice recognition device which can connect to or activate a wide range of computer-based equipment. [DAVI91, p. 34]

Voice systems can be speaker-trained or speaker-independent. Most voice systems are speaker-trained; the user must have training to understand the word-specific vocabulary required to operate the system, then they install the vocabulary by reading it into the system. On the other hand, speaker-independent systems have a limited special vocabulary and understand words stored from a pre-recorded pool of speakers. The users require minimal to no training to operate these systems. [DAVI91, p. 34]

Categories of voice data systems are continuous speech and isolated word. Continuous speech allows the user to talk at a normal speaking rate and records the voice patterns. Continuous speech can be used in either speaker-dependent or speaker independent systems. Research is being done in both of these speaker areas. Isolated word systems require a slight pause after each spoken word or phrase and can be tiring for the user. Continuous speech systems are usually more expensive than isolated word systems. [DAVI91, p. 34]

The biometric and voice recognition systems are based on measures of effectiveness, to use a certain level of confidence, to identify to the system that the user is who they say they are. These measures include enrollment time, verification time, percentage of "Class I Failures" otherwise known as "false rejections," and percentage of "Class II Failures" otherwise known as "false acceptance." [INFO94, p. 20] False rejection occurs when the system denies access to the authorized user and is measure by the "false rejection rate (FRR)." False acceptance occurs when the system allowed a person on the system when they should not have received access and is measured by the "false acceptance rate (FAR)." [MILL94, p. 197] These systems can not guarantee that the offered

characteristic will exactly match the stored digitize image, therefore the systems must be designed based on some confidence level that the requesting user is the genuine user. The system will be designed to compare the stored digitize image with the presented digitize image, make a decision based on the compared information to deny or allow further system activities to occur. [CART94, p. 403]

The cost of the biometric and voice recognition systems vary on the complexity of the hardware and the software to acquire the required biometric or voice information and the systems with which they will interface. Various pricing information can be acquired by contacting manufacturers and vendors of the specific technology that will meet the identified need.

b. Applications

Biometric and voice data technologies are used for security, identification systems, and access control applications, in areas such as banks, government installations, prison installations for prisoner identification, security and identification of truck drivers transporting various cargo, health spa membership, [DAVI91, p. 14] for time and attendance tracking [WEND94, p. 420], to list a few uses. Voice data technology can be applied in numerous other applications which include laboratory activity, material handling/processing activities, inventory control, quality control, forklift and inspection operations. It can be used to activate computer-based equipment, such as workstations, terminals, printers, scales, instruments, programmable logic controllers (PLCs) and conveyors systems. [DAVI91, p. 34]

c. Strength

The major strengths of biometric ID technologies are the availability of various biometric and voice recognition systems, many vendors to market these systems, and they provide security features to integrate with other technologies. [CART94, p. 403] In addition, the main strengths of voice recognition technology is it requires minimal training, it is real-time capture and entry of data while the operators are performing their

work, and it can be cost effective depending on its use. [DAVI91, p. 34] The major biometric ID technologies in use are the fingerprint and the hand geometry, and these systems interface well with personal computers systems. Biometrics and voice data are storable in digital form on various media to include bar code, magnetic stripe card, RF/ID card/tag, smart card, optical memory card, PCMCIA card, floppy disk, and magneto optical media. [INFO94, p. 20]

d. Weakness

Various weaknesses do exist for biometric and voice data recognition systems. These weaknesses include there are no standards established at the present time for biometric and voice data recognition systems [INFO94, p. 20], and the cost of the various systems can be high depending on application and the intended use of the technology.

2. Machine Vision Technology

a. Characteristics

Machine vision technology involves the use of computer systems to process and analyze image data from various manufacturing or material processing/handling operations. The electronic or machine vision system can use a video camera [DAVI91, p. 21], a high-resolution television camera, or an equivalent system [PALM91, p. 6] with signal processing circuitry to interface with a computer. Through complex software programs, the computer creates a digitized representation of the scene in its memory. The image data is used to assist an operator in making a decision about the scene. In addition, computer systems, using machine vision techniques, can facilitate decision making in operations without human intervention. [DAV91, p. 21]

The software programs used to process the digitized image use various algorithms to obtain the desired information. [DAVI91, p. 21] These software programs are typically complex and the associated hardware equipment is usually custom-tailored for the specific application. In addition, some form of optical marking is required for machine

vision systems to differentiate between externally physically similar objects. The optical marking can be a series of arbitrary marks or conventional characters, such as a bar code or OCR symbol, respectively. [PALM91, p. 6]

b. Applications

The various application areas include automatic identification, gauging, materials handling and sorting, measurement and quality inspection, robotic assembly, robot guidance and control, and natural and medical sciences. Various industrial applications include aerospace, automotive, food, drug, beverage, electronic, lumber, metals, rubber industries, [DAVI91, p. 21] and the postal service. [INTERMEC] Its automatic identification capabilities are used where more conventional forms of automatic identification systems, such as radio frequency can not be used. [DAVI91, p. 21] The area scanning technology of machine vision are ideally suited to manufacturing, processing, and in supply organizations, like the Postal Service, for sorting and tracking applications. The various postal services use area scanning technologies for letter mail, flat mail and parcel mail systems. A key feature of this technology is the systems are designed to read the symbols in any position or orientation. [INTERMEC]

c. Strength

The strengths of machine vision systems are they can operate without human intervention, they can be used with various technologies (e.g., bar code, OCR, etc.), they can be used where more conventional forms of automatic identification can not be used, they can facilitate decision making, and they can be used to monitor and control robotic activity. Machine vision can be used in various application areas. This technology also acquires the strengths of the associated media used in its applications.

d. Weakness

The weaknesses of machine vision technology are there are no standards identified for system development and implementation, they are typically complex systems to design, develop and implement, and the systems are more expensive compared to other

AIT systems. For example, the higher cost of a machine vision system is due to software complexity when compared to bar code technology, which has simplistic software used in the bar code systems. [PALM91, p. 9] This technology acquires the weaknesses of the associated media used in its applications.

I. HYBRID CARD TECHNOLOGY

Hybrid cards are cards that use multiple AIT resources on one card. Figure 2.10 is an example of a "hybrid" card with a magnetic stripe and an integrated chip on one card. Other technologies that can be used in some location on one card have been bar code, optical memory, RF/ID, and biometric technologies. [SEID93, p. 23]

J. SUMMARY

Automatic identification technology (AIT) card systems can originate from a variety of sources using a variety of media and enhancing technologies. This chapter discusses the technologies that are considered for card media technologies, other AIT resources, and the associated enhancing technologies that can be added to a card to enhance it functional capabilities. The various technologies discussed were bar code, magnetic
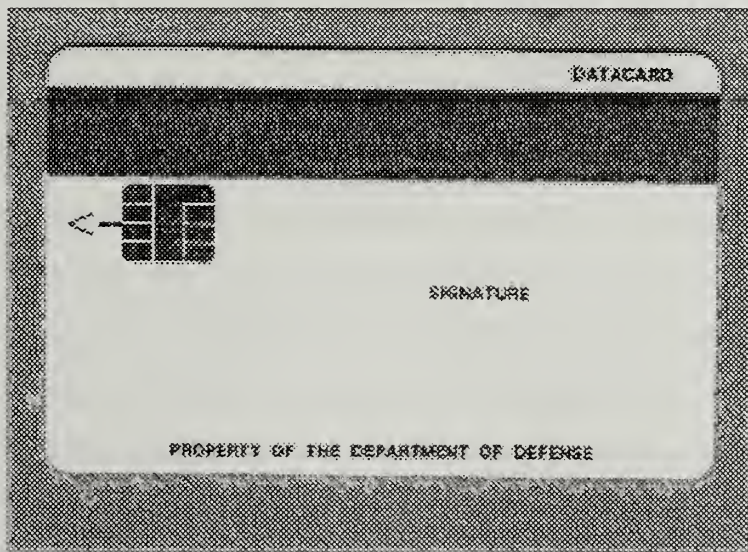
Figure 2.10: Example of a "Hybrid" Card Technology

stripe, radio frequency identification (RF/ID) including radio frequency data communication (RF/DC), optical card, smart card, super smart card, PCMCIA card, magnetic ink character recognition (MICR), and optical character recognition (OCR). The enhancing technologies discussed were biometric and voice data collection and machine vision. Each of these technologies have different operating characteristics, with various strength and weakness characteristics that must be consider for their use in various applications. For card applications, the card will be used in various environments, under various conditions, and for various purposes. The operating characteristics and the strengths and weaknesses of the various technologies must be considered when identifying, obtaining and implementing the technology for card application to obtain the desired AIT card system results. The strengths and weaknesses of the AIT technologies have been consolidated into tables and are located in Appendix A for a quick reference.

III. AIT CARD APPLICATIONS

AIT card technologies have been in existence for many years and have been applied in numerous applications. This chapter presents a brief discussion of a small sample of these applications. With a basic understanding of the various AIT resources, and how they function, the reader is encouraged to keep those concepts in mind as he/she reads how the technologies have been implemented. Even today, new applications for these technologies are being researched and developed. As these technologies and their applications continue to mature, they will have a major impact on how organizations and their processes will operate and be managed.

A. ACCESS CONTROL AND SECURITY

Access control and security systems are designed to protect land, buildings, office environments, and other areas or systems that require protection from unauthorized entry and/or use. The primary focus of these systems is protection with a secondary focus being ease of use for the legitimate users of the systems. The main components required for access control and security system operation are hardware/software, reader/writer system, and the card medium. These systems can consist of badge entry systems, various card systems with biometric and/or encrypted processing, and key storage devices. The card medium can be bar code, magnetic stripe, RF/ID tag/card, smart card, or optical card. The card can contain photo or digitized imaging, personal identification number (PIN) access, or some biometric digitized data (e.g., fingerprint, retinal scan, voice recognition) for user authentication to access the system environment. The stand-alone computer system typically requires the users to identify themselves for user authentication before granting access to the host system or activity environment. Important features of access control and security system administration is the various areas of access, day and time-of-day schedules, and levels of access that is to be granted to the user by the card system administrator. These are important features for access control to highly sensitive areas. [FMS90, pp. 6, 33, 54, 138, 165] Smart card systems can be programmed to perform

automatic log-on and log-off procedures for client to host system authentication for remote user access. [BROW88] Some card systems can be designed with encryption algorithms (e.g., Data Encryption Standard (DES)) for additional card security. [SFSC91] [SOLT94] The benefits achieved by these systems are access control and ease of use. The system can be secure to allow only authorized users and an access control log can be created and maintained. Through the automation of this activity, the system is easier to use and maintain than other non-automated systems. [FMS90, p. 138] Backup battery systems can be designed into the card system for off-line use in case of power outages. [FMS90, p. 165]

B.   CAMPUS CARD (STUDENT, FACULTY, SUPPORT PERSONNEL)

The campus card system has been implemented at many universities and colleges across the United States. The basis of this card system is to have the campus personnel carry one card that can be used for multiple campus applications, the "one-card" campus concept. Campus card systems have been designed with magnetic stripe, magnetic stripe with bar coding, and smart card technologies, and can include PINs, passwords, biometric, and voice recognition systems. These systems can be designed as stand-alone, turnkey systems which use specialized hardware (e.g., transaction processing units, card reading terminals for POS, door access) with the supporting software from specific vendors (e.g., proprietary systems) based on industry standard microcomputer systems and card readers. The systems can be designed to operate on-line or off-line. These card systems are versatile and can be sophisticated to meet various campus personnel needs. [FMS90, pp. 235-238]

Various campus card applications exist to meet the needs of the campus community, the students, faculty, and support personnel. Campus cards can be used for food services (in dining halls); student identification; access control (e.g., resident housing, laboratories); ticketing (e.g., concerts, theaters, cultural activities, recreation centers, and sporting events); health service; library services; laboratory equipment check-out; debit card purpose, in areas such as bookstores, dry cleaning, convenience stores, student unions, snack bars, welfare and recreation equipment rental, vending machines, laundries, and

copiers; tracking student information (e.g., transcripts, schedules); and other business services offered on campus. This list is not all inclusive, but is a small sampling of campus activities that can be supported with card technologies. [FMS90, pp. 235-238] Two military applications of campus card systems are the Falcon card at the Air Force Academy in Colorado Springs, Colorado and the Army campus card system at West Point, New York. [REBO94]

Campus card systems provide many benefits to the card users and the overall campus operation. They are convenient for the user to obtain services, for access control and for debit card purchases. The cards provide quick access to various systems which reduce time spent in waiting line, at vending machines and laundries, and reduce vandalism associated with cash-operated systems. Debit cards simplify book keeping, money management processes, and provide an audit trail to track expenditures and report balances. Use of the card can increase purchases made at the campus stores and other campus facilities, thereby increasing campus revenue. [FMS90, pp. 235-238]

C.   DOCUMENT STORAGE CARD

AIT card technologies have been researched for their use as document storage cards. Document storage system in this context includes published books, digital microfiche, publications, and manuals. The main two technologies which have been tested for document storage applications are optical (laser) card [LATA85] and PCMCIA cards [RIST93, p. 267] Research has been conducted with storing and publishing encyclopedias and other books on optical (laser) card. [LATA85]

D.   ELECTRONIC CERTIFICATION SYSTEM

AIT card technology has been use in applications that require some means of electronic certification for authentication of the user before any further system activity can be authorized. An example of a certification system is the Electronic Certification System (ECS) that uses electronic signatures to certify Federal Program Agencies (FPA) payments to the Financial Management Service. Smart card technology is use in this system. The

Certifying Officer is issued a smart card and a PIN by the Washington Financial Center. When the Certifying Officer authorizes payment, the smart card, which contains a cryptographic key, is used to generate a Message Authentication Code (MAC) for the payment request schedule. The system, which operates by hardware based encryption technology (e.g., DES), uniquely identifies the user who signed the payment request, verifies that authentication of the MAC, and accepts the payment request. The benefits of the system included increased security of payment processing and reduced schedule preparation time. [FMS90, p. 40]

E. ELECTRONIC TICKET COLLECTION (ETC) (SPECIAL EVENTS)

Card technologies have been used as a ticketing mechanism to gain access to various events. On college campuses, students and faculty use their magnetic stripe card for entry to sporting events, concerts, plays, theaters, cultural events, and other college sponsored activities. [FMS90, p. 237] In Seville, Spain, season ticket holders use their smart cards and a fingerprint as their admission ticket to various events. [FLOO92]

F. EMPLOYEE CARD (TIME, ATTENDANCE)

The purpose of the employee card is to track time and attendance data of employed personnel for payroll and leave accounting. Each employee is issued an identification badge, or card, typically with the employee's photograph, identification information, and possibly some activity information. The badge or card media can be bar code [FMS90, p. 25], magnetic stripe [FMS90, pp. 22, 23, 58, 64], smart card [WON91, p. 5] or RF/ID technology that will interface with a scanner or read/write system. The systems are designed to collect check in/check out time and attendance information, perform required time keeping functions, and transmit these transactions to the host computer system for processing. The host computer will track the employee's hours worked and the accrued leave information for personnel payroll tracking, for management and resource control reports, and produce error listings. This information can be consolidated with other

68

employee information in a personnel record of employment history for each employee. [FMS90, pp. 22, 25]

A military application of time and attendance tracking can be for management of reserve personnel drill participation and drill payment. From an established database, the reservists are authorized and scheduled to perform drills. The system is designed to record the date and sign-in time when the reservist is scheduled to report to drill and can record a "payment" code when the drill is completed, or it can automatically enter an "unexcused" code when the member has not reported for the required drill. [FMS90, p. 58] Other information can be maintained on the card and in the database for additional reserve management applications.

Many benefits of automating time and attendance tracking systems have been noted. These benefits include reduced operating cost, reduced data entry errors, reduces labor costs, efficient process to automate the manual operations associated with employee time and attendance information processing; reduced payroll preparation time, timely final data transaction posting; supervisors, timekeepers and employees can have immediate access to time and attendance information; and it can be used as an effective decision support tool at all management levels. [FMS90, pp. 22, 25-26] In addition, better internal controls can be designed in the system to meet established regulations. [FMS90, p. 58]

G. FINANCIAL

AIT card technologies can be used in many financial applications. The financial application areas are defined into more specific application areas to identify the card technologies that have been applied. The specific application areas include accounting systems, automated teller machines (ATMs), credit collection/authorization, electronic benefits transfer (EBT), and prepaid cash (e.g., POS, debit, stored value card).

1. Accounting Systems

AIT card technologies can be applied in accounting systems management. These accounting systems can include tracking pay, allowances, and to monitor debit and credit transactions by individual accounts. An example of this application is the smart card

program at the Marine Corps Recruit Training Center at Parris Island, South Carolina. In order to better account and issue pay to the recruits and reduce the administration and material costs associated with the administration of the paper coupon system, the Marine recruits received their pay on a smart card. The smart card is used to make cash withdrawals and purchase transactions at various base facilities. The transaction information is transmitted from the POS terminal to the host computer system in the Exchange Controller's office. The benefits achieved from this smart card systems are better account administration and cost savings of the card based system versus the paper based system, update and reuse of the smart card, built-in security of the card is achieved with PIN identification to minimize theft, and purchase transactions are faster and they can be tracked. [FMS90, p. 70] Bar code technology has been used for payroll accounting, food services, and other accounting needs. [FMS90, p. 132]

Magnetic stripe card technology has been effectively used for the financial management of imprest fund or "petty cash" fund accounting. The magnetic stripe cards were used by imprest fund cashiers for cash transactions through established ATM networks. The benefits achieved through this system were improved management of the imprest fund and quicker cash transactions compared to the paper based systems. [FMS90, p. 42]

2. Automatic Teller Machine (ATM)

ATM systems have been established and effectively used with magnetic stripe technology since the late 1960s. These systems in the banking industry became an economical means for processing patron requests for cash transactions. [SVIG87, p. 21] With the well established infrastructure of the ATM technologies, corporations have been forging forward to research and develop the next generation ATM machines which will support smart card use. The manufacturers are designing upgrade kits for ATM systems which include smart card readers. These systems support and protect the banks' investment in ATM systems. [HOFN92]

3. Credit Collection/Authorization Card

AIT card technologies can be used in various credit collection and authorization programs. These programs typically are developed using magnetic stripe card technology. An example of a credit collection/authorization card system is the Government-wide Commercial Credit Card, otherwise known as the "International Merchant Purchase Authorization Card (I.M.P.A.C.)." Once purchase limits are checked and authorization is given to the card holder, the I.M.P.A.C. card can be used to make small purchases under an established Delegation of Authority for official government use. [FMS90, p. 10]

4. Electronic Benefits Transfer (EBT)

AIT card technologies can be used in many electronic benefits transfer (EBT) programs for public assistance programs. The EBT programs include food stamp programs; Aid for Families with Dependent Children (AFDC); Women, Infants, and Children (WIC); child support benefits; foster care program benefits; medical benefits program; Social Security Income (SSI); and unemployment benefits program.

a. Single and Multiple EBT Programs

EBT programs are being implemented on various card system which can support one program or a combination of public assistance programs, such as food stamp, AFDC, WIC, child support benefits, foster care, and medical benefits program. Magnetic stripe cards, with PIN verification and/or photograph identification, are the most used systems with the card issued to each participating household. Bar code and smart card systems can be used for various human services and support programs. [FMS90, p. 99] [SANT92] The recipient can utilize the benefit card to acquire food stamp benefits as on-line debits at authorized POS terminals and participating food retailers, acquire cash assistance payments through ATMs, and acquire medical benefits after medical providers access eligibility information and receive authorization numbers, either electronically through POS terminals or by telephone communications. [FMS90, pp. 88, 99, 100, 110, 211] [WON91, p. 11] Smart card systems have an added capability to be used in off-line

EBT. The major benefits achieved by these systems are cost savings for automated systems in comparison to the cost associated with maintaining and administering paper-based systems and improved benefit delivery to recipients. [IACO91]

b. Supplemental Security Income (SSI)

The Supplemental Security Income (SSI) Payment program was a pilot program implemented by the Department of the Treasury, the Financial Management Service (FMS), and the Social Security Administration (SSA) in 1989. The program was developed to improve the quality and service in the delivery of SSI benefits payments to qualified recipients through the use of a magnetic stripe card program. The recipients would use their magnetic stripe card at designated ATM and POS terminals to withdraw their benefits. [FMS90, p. 48]

c. Unemployment Insurance Program

The Electronic Benefits Distribution System was a pilot program administered by the Employment and Training Administration of the United States Department of Labor. The program was designed for unemployed personnel to use a plastic magnetic stripe card to obtain unemployment benefits payment. The unemployed personnel would certify their eligibility for unemployment benefits using a touch tone phone interfacing with an automated audio response unit. The caller would enter their required eligibility information and a PIN and the automated response unit would respond with the benefit information. The recipient would then access their weekly payments by choosing the payment option of direct deposit to a bank account, traditional check transaction, or use of an ATM or POS system. [FMS90, p. 221] In Canada, smart card technology has been explored for an unemployed client use to obtain employment information and benefits payments. [MCCR92]

5. Prepaid Cash/Debit/Stored Value Card

Various terms for prepaid cash have arisen based on its applications. In AIT card applications, where the card can be assigned some cash value and can be used at various point of sales terminals, in pay telephone applications, or in vending machine systems, the prepaid cash cards have also become known as debit cards or stored value cards. The concept of the prepaid cash card is based on "pay before" use, and it is a safer form of carrying cash. The card technologies used for prepayment applications include bar code [FMS90, pp. 117-118], magnetic stripe [FMS90, pp. 44, 77], and smart card [MART89].

In use, the prepaid cash card can be purchased with a specific dollar value or the card can be assigned a dollar value through an accounting system. When the prepaid cards are purchased for some specific dollar amount, the dollar value is decremented with each use until there is no remaining cash value, and the card can no longer be used. Examples of applications that use this prepaid cash card are transit systems and pay telephone systems. Other prepaid cash card systems are designed for debit/credit use where the cash value maintained on the card can be debited and credited. These prepaid card systems result in additional use of the card technology in many debit applications (e.g., campus card, benefit card). The benefits acquired from prepaid cash card systems are convenience to the user, reduced need to carry loose change, less chance for theft and vandalism, less machinery maintenance, and reduced need for vending personnel to handle and be held accountable for money. [FMS90, pp. 16-17, 117-118] In addition, while most prepayment card systems use proven magnetic stripe technology, smart card systems can provide more security and have greater potential for additional applications than magnetic stripe card systems. [FLOO92]

The 1990s has been an excellent period for prepaid debit cards to be marketed as a payment tool. Banks and financial institutions are offering programs and establishing on-line electronic funds transfer (EFT) networks (e.g., MasterCard's Maestro, Visa's Interlink, MAC) to strengthen their relationship with their customers and offer value-added benefits for use of their services. Banks are restructuring their delivery system to facilitate self

service for added customer convenience. [MOOR92] Some EFT networks are issuing smart cards with a magnetic stripe to be use in off-line and on-line debit card applications. Merchant and customer acceptance will drive the trend for prepaid debit card use. [PUNC92] Non-cash transactions, such as use of prepaid debit card, are being encouraged to combat money laundering. As the use of prepaid debit cards increases, regulations, technologies, and card and data transaction protection schemes need to be developed and implemented to protect consumers from potential abuse and error that can occur with these systems. [SAMU92]

H.   HEALTH SERVICES

AIT card technologies have been applied in health/medical service systems. The application of card technologies in this area include use as a health service card for patient care and monitoring, as an insurance card for health related matters, and as a pharmacy card.

1. Health Services Card

In 1984, France and Germany pioneered the use of smart card technology for health care administration. [DCPR84] Today, various AIT card technologies have been identified and applied as health service cards in the area of health care administration. The card technologies applied in this area include bar code [PALM91, pp. 205-206], magnetic stripe [FMS90, pp. 144-145, 163], RF/ID [CUSH94, p. 346], smart card [DANI91], and optical card [INFO94, p. 13]. The health care card is designed to provide access to identify a patient and to track personal health information at various medical treatment locations. Patient can even be monitored in the medical facility with the use of a RF/ID technology. [CUSH94, p. 346] Medical history, allergy information, lab results, X-rays and other medical information can be stored on the card and/or stored in a centralized database. A physician can use and review a person's medical card for instant access to important medical data to facilitate and support diagnosis and treatment. In addition, the physician and/or medical treatment facilities billing systems can be connected through networks with

insurance delivery institutions for insurance claim processing. [STEI87] Some health care card systems are designed to contain the minimum amount of information possible on the card (e.g., the information that remains constant) to reduce the need to replace the card or require multiple cards for various applications. These card systems are designed to interact with a database to retrieve the required medical information or determine benefit eligibility status of the member seeking medical services. [FMS90, pp. 144-145] The Department of Defense (DoD) has initiated a multi-technology automated reader card (MARC) program which is a credit-size card that contains a DoD Standard Code 39 bar code, an updatable magnetic stripe, an integrated chip, and embossed and printed information. The card will be used for various military applications to include military personnel health care activities. [KIRS94, p. 623]

2. Insurance Card

AIT card technologies have been implemented and used as insurance cards. Magnetic stripe and smart card technologies have been used to assist doctors and other personnel in the health care system who process medical claims for payment. Claim services have developed where the physicians and medical personnel swipe the magnetic stripe card or insert the smart card into a special processor that links to the claims processing service for speedy and paper-less transactions. [JOHN91] Many people benefit from these card services, to include the physicians, the insured and the insurers. These benefits include customer identification and eligibility status determination, electronic claims processing, and claims transaction tracking and auditing. Some concerns of these claim processing systems do need to be addressed, such as hardware and software standards, liability issues for cards having incorrect data, and the total system implementation costs. [DANI91] An example of this system application is Medicaid program administration to reimburse health care providers for their services to eligible recipients. [FMS90, p. 163]

3. Pharmacy Card Applications

AIT card technologies have been applied in various aspects of pharmacy applications. A smart pharmacy card has been designed to be used with a drug interaction database and existing pharmacy systems to assess prescribed drugs used by the card owner and prevent adverse chemical interactions of drugs that should not be taken together. The card will contain the patient's drug information, drug allergies, and disease information as needed. The software is designed to send on-screen warnings and provide other information to handle conflicting information that could affect the card holders' medical status. [WON91, p. 13] Magnetic stripe pharmaceutical card system have been developed for eligibility and claims status verification and adjudication, track medication dispensing information, and process bill payment. [FMS90, pp. 206-207]

I.   LIBRARY CARD SYSTEM

Various card technologies have been used for library systems, which include bar code, RF/ID, smart card, and optical card systems. Bar coded library systems have been successfully applied at university and college campuses. The bar code on the campus card is used at the library for access to books and other related materials. [FMS90, p. 196] RF/ID systems are designed for electronic article monitoring in library applications. [CUSH94, p. 346] Smart cards have been used for library record applications. [SMIT87] The optical card has been effectively used as a library card where the owner of the card receives library services, to include the use of a personal computer, an optical scanner and the CD-ROM disk library with the associated software for each system, and printer support. Patrons can have a PIN assignment on their optical library card to make it more secure from unauthorized patron use. [SPEC93, pp. 218-219]

J.   LOGISTICS

AIT card technologies have been used in the automation of many logistics systems. Under the title of "logistics systems" is a broad range of application areas which includes inventory control, tracking of repair parts, fuels management, and mobility applications.

The card technologies used in these application areas are bar code [FMS90, p. 60], magnetic stripe [FMS90, pp. 255-257], RF/ID [FMS90, pp. 257-258], smart card [FMS90, p. 28], and optical card. [CAPA94, p. 294]

1. Inventory/Material Control

The inventory control programs are designed to automate receiving, storing, tracking, and shipping of various material goods. Examples of these items are high value/critical items (e.g., weapons, ammunition), proprietary and DoD classified items, and hazardous and/or sensitive items (e.g., nuclear and medical wastes) from various military and commercial activities. [FMS90, p. 20] These systems automate inventory and manifest information processing by creating electronic manifests that accompany the shipment of material from one activity to another or used for warehouse tracking operations. The electronic manifest should be stored on a durable card technology that can survive various shipping conditions. At the destination, the electronic manifest information is uploaded to a computer and a list can be generated (via the computer system) to identify the items shipped, note any discrepancies, and produce the required management reports. These systems are flexible and can be configured for various operational environments to include military, industrial, and agricultural applications. Examples of the various inventory control programs are the Army Material Control (AMC) project [FMS90, p. 63], which uses RF/ID and smart tags to track the shipment, storage, and retrieval of materials based on a specific pallet number [FMS90, p. 38]; Logistics Applications of Automated Marking and Reading Symbols (LOGMARS), a DoD program in which DLA participates, is a program designed to test smart card and bar code technologies for in-transit inventory control applications associated with military supply systems [FMS90, p. 69]; the Defense Logistic Agency (DLA) Automated Manifest System (AMS) uses RF/ID and optical card technology to track the supply and transportation manifests of loaded pallets and seavan shipments to various operational areas [CAPA94, p. 297]; the hazardous waste material tracking system uses RF/ID and bar code technology [FMS90, pp. 60-61]; Automatic

Equipment Identification (AEI) uses radio frequency (RF) transponder systems for tracking shipping containers within the maritime-industry, [FMS90, p. 30] and the In-Transit Visibility (ITV) and the Total Asset Visibility (TAV) programs which use microcircuit technology in logistics applications (MITLA) resources. [SHAR94]

2. Fuel Control

Fuel control programs are designed using various AIT card technologies. Magnetic stripe or smart card/smart key systems are the main AIT resources used in fuel control systems. The magnetic stripe and smart card systems are used to activate fuel pumps, automatically collect fuel data, pricing information, and transmit this information through the card reader to a host computer system for customer billing. [FMS90, p. 198] Smart cards are being used at truck stop fuel transaction station. Smart card system can be used for added access and security at fuel stations. [FMS90, p. 160] The benefits of these card systems in automated fuel transaction stations efficiently move vehicles through the fueling islands, reduced billing errors, [SCST93] and reduced labor costs. [FMS90, p. 198]

3. Mobility

Smart card and bar code technologies have been used military mobility applications. The Automated Mobility Processing System (AMPS), designed by the Microcircuit Technology in Logistics Applications (MITLA) program group, automates the process to mobilize troops and their critical supplies in respond to world wide deployment requirements. These card systems used hand-held terminals to read and revised data as necessary. Strength reports are produced from these systems to identify personnel and material/equipment shortfalls. The benefit of this card system was speed, efficiency, and accurate tracking of recall unit personnel and their equipment from their duty station to the points of embarkation and debarkation. [WON91, p. 7] The Army Soldier Readiness Card (SRC) and the DoD MARC programs are being evaluated for unit personnel and equipment mobility/readiness processing. [KIRS94]

K.   MANUFACTURING OPERATIONS

Manufacturing and maintenance activities can effectively use card technology for tracking component parts in design, repair and at the quality assurance points. The systems can also be established to track the life cycle management of various products. The card technologies used in these applications include bar code [PALM91, p. 198], RF/ID [FMS90, p. 65], smart card [SANT92], and optical card [KAEB92]. System application include manufacturing [SANT92] and vehicle history maintenance records [KAEB92]. Examples of military applications include the Electronic Scheduled Removal Component Card (SRCC) used in the Navy aviation maintenance activity to record maintenance history for aviation components [FMS90, pp. 36-37], radio frequency tags used in small track vehicle areas at the Red River Army depot [FMS90, p. 65], and RF/ID tags used in shop flow monitoring at Kelly Air Force Base, Texas. [REBO94] These systems are designed to provide reliable data storage of information on the tagged component. An example is the SRCC is a customized microcircuit card (smart card) that holds 8K bytes of data and is attached to the component in an enclosed plastic case that interfaces with a specially designed reader. The reader systems interfaces with a laptop computer so the users can update the cards or obtain data as needed. Upgrades to this system were achieved by using 10K contactless tags and portable readers. The benefits received from these systems are reduced information processing requirements for manufacturing and maintenance personnel and improved availability and accuracy of data. [FMS90, pp. 36-37]

L.   MARKETING OPERATIONS (TRADE SHOW, CONVENTION)

Card technologies have been used in marketing applications and for data management and registration processes at trade shows and conventions. An example of card use in this area is the Expocard [LAUG93] and the CardTech/SecurTech card. Smart cards were used at these conferences for registration processing, promotion of the technology, acquiring resource materials, and to track visitor transactions. Many benefits can be recognized with the use of this technology to include visitor/registrant convenience

to expedite the registration process, access control to the convention area, effective tool for visitor-exhibitor communication to acquire information and obtain sales/buyer leads, data management of convention processes, demographic and survey information collection, identification of the type of audience attending the conference/convention, track various activities (e.g., luncheons, host dinners, seminar attendance), and use as a conference/ convention promotion tool to demonstrate leading edge technology, the products, and the various applications of the products (e.g., debit/credit card, health card, retail, banking, and various other applications). [LAUG93]

M.   PERSONAL IDENTIFICATION AND MANAGEMENT

Various card technologies are used for personal identification applications. The present card technologies used for applications in this area include bar code, magnetic stripe, RF/ID, smart card, and optical card. Proximity cards are also used which have similar characteristics to RF/ID or contactless smart card systems. These card technologies can be used with PIN, photographs, biometric devices, voice recognition systems, and digitized signatures. The majority of these cards are used for access control, benefits programs, or medical applications, where personnel identification is extremely important. [FMS90, pp. 255-259]

N.   RESOURCE MANAGEMENT

Various resource management programs have implemented card technologies to facilitate program administration. The California Department of Forestry and Fire Protection researched smart card use for check-out/check-in of various fire fighting resources [FMS90, pp. 96-97], the Wisconsin Department of Natural Resource tested smart card technology to automate and modernize their licensing systems (e.g., hunting, fishing) [FMS90, pp. 226-227], and the Department of the Air Force researched smart card and RF technologies for the Military Dog Management Program. [FMS90, pp. 55-56] Numerous benefits were noted with the use of card technologies in these application areas.

1. Forestry

The California Department of Forestry and Fire Protection tested the use of smart card technology to provide fast, reliable check-out/check-in of fire fighting resources (e.g., equipment, vehicles, aircraft, and people) and transmitted this information over a network into an integrated database for base management's use for near real-time operational planning, logistic support, and direct resource use. The smart card system could capture and transmit data to the database in seconds vice hours. Various information could be stored on the smart card to include personnel information, emergency notification information, certain medical data, personnel qualifications, agency required information, vehicle information, and equipment information. [FMS90, pp. 96-97]

2. Licensing

The Wisconsin Department of Natural Resource researched a licensing smart card system managed from a centralized database that contained customer information on the various types of licenses purchased. The customer's licensing information would be on one smart card vice issuing various licensing stamps (e.g., salmon, trout, turkey, small game), license type (e.g., fishing, hunting), or permits. Durability of the card and the use of hand-held reader systems in this application were being researched. Program benefits included a modernized methods of sales and issuance of permits and licenses which resulted in better customer service, reduced state licensing operation costs, and better cash flow management associated with these resource systems. [FMS90, pp. 226-227]

3. Military Dog Management Program

Department of the Air Force researched the use of smart cards and radio frequency identification for the Military Dog Management Program, which trains dogs for use in Patrol, Drug Enforcement, and Explosive detection. The program was designed to have a passive radio frequency/microcircuit device in a dog's collar to assist in positive identification of the dog. The data maintained on the dog would include purchase and receipt, kennel control, location, training progress, diet record, veterinary record, and shipping. The benefits of this program include an automated program for military dog

management and it eliminates the need to read the dog's identifying tatoo for the various activities. [FMS90, pp. 55-56]

O.   RETAIL APPLICATIONS (RETAIL, VALUED CUSTOMER)

Many card technologies have been applied in retail applications. Retail applications cover a broad range of areas to include, but is not limited to, valued customer programs, frequent shopper programs, discount programs, and supermarket purchases. The card technologies used in retail applications include bar code [PALM91, p. 203], magnetic stripe [MURP92], RF/ID [CUSH94, p. 346], smart card [GATE90], and optical card [KAEB92]. Debit card use of magnetic stripe technology has been used for retail application and it has been growing in recent years. Financial institutions (e.g., banks, credit card companies) have realized the potential of this application and are taking some action on what their roles will be in the debit business. Nationwide and regional networks are arising to spur the use of debit card services at the point of sales in these retail environments. The main retail areas where these services have been implemented are convenience stores, supermarkets, and gasoline stations with possible future retail areas being discount stores, dry goods stores and dry cleaning services. [KASS92] European countries have used smart card technology in supermarket check-out counter activities. Smart card application in this area can promote customer loyalty and can be used for target mailings. The benefits of these systems are automated retail systems can provide useful information to management by collecting the shopper's demographic information and shopping behavior for future business planning and these card systems can be designed to maintain an audit trail of transactions. [GATE90]

P.   SERVICES

The service sector has many applications where AIT card technologies have been implemented. The service sector include government, state and county sponsored and operated programs. These programs include the United States Department of Agriculture (USDA) applications, farm quota applications, and other agricultural applications; education/training/job placement services; pay telephone; post office operations; and

school lunch programs. The AIT card technologies implemented in the service sector include bar code [INTERMEC], magnetic stripe [BASS93], RF/ID [CUSH94, p. 347], smart card [WON91, pp. 9-11], and optical card [BASS93].

1. Agriculture/USDA/Farm Quota System

Various AIT card technologies have been applied in agricultural applications. The two main AIT resources used in agricultural applications are RF/ID and smart card technology. RF/ID has been effectively implemented in animal identification applications, to include livestock feeding programs, livestock movement and control, milk production records, slaughterhouse operations, research and testing data collection, and to monitor various livestock breeding cycles. [CUSH94, p. 347] Smart card technology has been used by the USDA's Agricultural Stabilization and Conservation Service (ASCS) to automate the program management, oversight and payment for the production of various agricultural products (e.g., peanut and tobacco marketing). Production information was written to the smart card. The smart card would be read at the smart card terminal connected to personal computers at the buying points. The marketing record at the buying point would be transmitted to ASCS for recording and payment processing. The benefits of this smart card program were reduced costs, reduced paperwork processing, legal documents in electronic form, and the reduction of the human errors associated with non-automated processes. [FMS90, pp. 2-3] [WON91, pp. 9-11] Smart cards have the advantage of improved security when transferring information from one USDA agency to another. [HERM91]

2. Educational Service/Training/Job Placement

Card technologies have been applied as educational service, training and job placement card. The main card technology chosen for this application was the smart card. The smart card can be used to maintain an individual's record and assist the individual in obtaining education, training, and job placement services. The individual card is used as a distributed database that can interface with a microcomputer systems to obtain information on available education/training/employment programs; assess individual's education level,

training, skills, and experiences; identify a plan of action for future employment; identify and apply for services when eligible; and receive payment authorization to the service provider. An example of this type of program is the Michigan Opportunity System (MOS), which was the model program for other states to use when implementing education and employment-related services. [WON91, pp. 9-11]

3. Pay Telephone (Cashless Telephone Card)

Europe and Japan have used card technologies in pay telephone applications for many years. These systems are designed as debit card or cashless card operations where the purchaser buy a card of a particular value. When the card is used for telephone services, the value of the card is decremented based on the amount of service used. With each use of the card, the appropriate value is decremented until the cash value of the card is zero. The card technologies used for this debit card application are magnetic stripe, smart card, and optical card. [BASS93] Smart card telephone systems have been integrated with satellite communications and implemented on maritime industry vessels for ship-to-ship and ship-to-shore communication. [TFLO91] In the United Kingdom, card-operated cellular telephone services have been implemented. [MORA91] Many benefits can be realized with the use of card-operated telephones to include the reduced risk of vandalism; the reduced maintenance cost with fewer moving parts, which increases service capability and system reliability; reduced system operations costs, by not having to pay personnel to collect the cash in the cash-operated telephones; increased revenue; and the commercial advertising potential of the card. [BAND91] The additional benefits of smart card telephone systems are increased security, and increased data storage and processing capability when compared to magnetic stripe card systems. [FONT93] In addition to cash-less cards, companies are developing smart card adapters, which contain a smart card reader/writer and a modem, to be used with touch-tone telephones. These adapters can be plugged into a standard telephone line and the smart card can be used in the system to verify the user and process transactions. [AMSC93]

4. Parcel Tracking and Post Office Operations

AIT resources have been used for parcel tracking, to automate post office operations, and for stamp purchases. RF/ID technology has been used for parcel tracking, to include tracking Federal Express, UPS, US mail, and airline baggage. [CUSH94, p. 346] Bar code technology and machine vision systems have been used to automate post office operations. The automation of these post office operations requires inspection and sortation of various mail items (e.g., letter mail, flat mail, parcel). These systems are designed to read various bar code symbologies, in any orientation, with a high resolution camera. The camera system is interfaced with a computer system that has sophisticated software to control the mail sorting process. [INTERMEC] Magnetic stripe technology is used to purchase stamps over the telephone. Use of a MasterCard, Visa, or Discovery card information transferred over the telephone when the stamp purchase request is made initiates the process. When the debit transaction of the credit card account for the stamp purchase from the financial institution to the Postal Service occurs, the Postal Office mails the stamps to the customer to complete the transaction. The benefits achieved with these systems include improved parcel tracking and location, reduced labor costs, improved customer service, and improved system operation. [FMS90, p. 24]

5. School Lunch Debit Card Program

Magnetic stripe card technology has been used in the development and implementation of a school lunch debit card program. The card program is designed to improve the overall school lunch process, to reduce the time the student spends in the lunch line, to reduce the time the teacher spends doing daily lunch information and money collection, for determining the quantity of meals to produce and accurate meal reporting, for improved record keeping of student meal status, and the associated computer system can provide daily, weekly, and monthly reports as needed. [FMS90, pp. 112-113]

Q. TRANSPORTATION

AIT card technologies have been applied in various transportation applications. The transportation applications include driver license processing, vehicle registration, vehicle tracking, electronic toll collection (ETC), traffic control operation, and weigh station operation. The card technologies applied to these applications include bar code [FMS90, pp. 133-134], magnetic stripe [MURP92], RF/ID [FMS90, pp. 136-137], and smart card [WON91, pp. 12-13].

1. Driver Licensing/Vehicle Registration/Vehicle Identification

AIT card technologies are effectively used in the vehicle-related applications. The vehicle-related applications include driver licensing, vehicle registration, and vehicle identification. The card technologies used in these vehicle applications include magnetic stripe technology [FMS90, p. 102] and RF/ID [CUSH94, p. 346]. Magnetic stripe technology is being used on the driver's license/identification card to facilitate driver license processing, to reduce the man-hours associated with manual data collection and paper handling processes, and for quick access and retrieval of driver identification and traffic safety information when needed. The information on the magnetic stripe is encoded and encrypted, which when swiped through a card reader/writer, will allow access into the Department of Motor Vehicle (DMS) database. In addition, encoding and encrypting the data on the magnetic stripe makes it more difficult to alter. Other technologies used on the driver's license include a photograph and a fingerprint. [FMS90, p. 102] Magnetic stripe technology has made vehicle registration easier by taking the existing MasterCard or Visa magnetic stripe credit card and use it in a vehicle registration system similar to an ATM machine. The system requests certain personal, vehicle, and insurance information, processes this information, bills the credit card, and issues the license plates, registration forms, and billing information to the customer. [FMS90. p. 218] RF/ID has been used for vehicle identification number (VIN) tags that can be use for various applications to include tracking the vehicle if it is stolen. [CUSH94, p. 346]

2. Electronic Toll Collection (ETC) (Road, Bridge, Bus, Train)

AIT resources have effectively been used in electronic toll collection applications. These applications areas include road tolls, bridge tolls, airport terminal tolls, train and bus tolls (transit tolls), and parking tolls. The AIT resources that have been applied to electronic toll collection systems are bar code [FMS90, pp. 133-134], magnetic stripe [MURP92], RF/ID [FMS90, pp. 257-258] [REBO94], and smart card [FLOO92].

The type of AIT card technology used for toll collection system will have a large impact on how the system is implemented, operated and maintained. Electronic toll systems that use bar code, magnetic stripe, and contact smart cards will require the patron to take some action to use the system. For example, toll road collection system that use bar coded cards will required the patron to have the card scanned, the scanned information will be transmitted to a host computer system that will bill the patron for the toll road use. Bar coded cards can be used to identify the toll collector lane assignment and can be used by technician personnel to track lane equipment maintenance. [FMS90, pp. 133-134] Most metropolitan/regional transportation systems use magnetic stripe cards for transit fare collection. Magnetic stripe transit tickets are typically prepaid ticket based on origin to destination information. The cardholder purchases the ticket and inserts it into a reader mechanism for transit system access. Smart card technology has been used in some regional transportation systems. An example of this application is the Payment and Control Information System (PCIS) developed for the Northeastern Illinois Regional Transportation Authority (RTA). This smart card system is designed for mobility-limited riders to obtain transportation services in the RTA region and be automatically billed for the services. [WON91, pp. 12-13] Companies are developing next generation ATM machines designed to support smart card use, which can be use in airline reservation systems. [HOFN92, p. 24] In addition, smart cards and magnetic stripe cards with prepaid value can be used for parking fee collection. [MURP92] [TORE93]

RF/ID tags and contactless smart card technologies can be used in electronic toll collection system applications. These systems are usually designed with passive toll tags

(e.g., transponders), transmitting and receiving equipment (e.g., interrogators, antennas), and a host computer system. The RF tag or the contactless smart card is located with or on the vehicle. The interrogator is located at the toll booth. As the patron uses the designated toll booth, the system identified the patron's tag, verifies and validated the tag's account at the host computer system, and deducts the toll charge from the patron's prepaid account. [FMS90, pp. 136-137] In addition, some transit organizations use contactless technologies to track and monitor performance and location of commuter bus services. Reading systems and antennas are installed at bridges, overhead signs, and other existing structures to track traffic movement. The bus movement is transmitted to remote computers used by the Port Authority. During peak traffic periods, information can be provided to bus operators to facilitate bus movement. In this operation, the contactless tag can be used to maintain maintenance and other information on the tagged item. [FMS90, p. 179] For toll operations, the bus identification code is transmitted to the associated computer system to record the transaction and debit the prepaid toll account maintain by the bus operator with the Authority. [FMS90, p. 182] Contactless tag systems can be used for parking fee collection and vehicle access control. [CUSH94, p. 346]

These systems provide many benefits to the patrons of these services. The benefits are reduced lines, reduced traffic congestion, better service, no cash transactions which reduced theft, less chance of errors, and faster toll traffic processing. These system are efficient, easier to use and manage, and they report fees and collect toll payments. [FMS90, pp. 133-134, 136-137, 182]

3. Weigh Station Processing

AIT resources has been tested for use in vehicle weigh station processing. Los Alamos National Laboratory in New Mexico designed a radio frequency license plate system to be use to electronically track and monitor commercial vehicle movement within the state and its ports-of-entry. Owners of vehicle participating in this program registered and licensed their vehicle in New Mexico, follow established New Mexico Vehicle Code,

and are in compliance with New Mexico Weight Distance and Special Fuels Taxes. Participating vehicle would not have to stop at port-of-entry, but would transmit information as they pass port-of-entry stations. This application reduced the vehicle congestion at the entry ports, reduced the port-of-entry personnel workload, and reduced delays in shipment. [FMS90, p. 167]

R.   OTHER PRODUCT APPLICATION

Card technologies can be used as a product, in addition to their use as a data storage/ data carrier media in various applications. With the increasing data storage capability of the card technologies, and the logic capability of smart cards, increase uses of these card technologies from a product perspective can be identified.

1. Modem/Fax Applications

Card technologies have been used as modem/fax products. The main card technology used in this capacity has been the PCMCIA card. PCMCIA modem card provides data transfer at 2,400 bps, 9,600 bps and 14,400 bps, with 14,400 bps modem cards having potential data transmission rates of up to 57,600 bps.

2. Network Interface Applications

Card technologies can be used in network systems as a local area network (LAN) adapter card or as a secure card to obtain access to a network system. PCMCIA card technology is used as a LAN adapter card. With the use of the PCMCIA LAN adapter card, notebook personal computers can be connected to the office network. [TABI93] A smart card can be used to access a network. The microprocessor capability of the smart card can be synchronized with an access control module (ACM) on a host computer system. The smart card and the host computer system synchronously calculate new passwords. When the user logs onto the host computer system, the user must enter the access code displayed on the smart card and a PIN for user identification to gain access to the system. [ROTH93]

3. Secure Telephone Unit (STU)

The smart card concept has been used in smart key applications. An example of a smart key application is the Secure Telephone Unit (STU) and the smart key, a KSD-64A, used to activate secure telephone communications between STU systems. The KSD-64A is a 64K bit portable data storage and transfer device in a plastic casing shaped like a physical key. Twenty-eight gold-plated contacts provide the interface between the KSD-64A and the STU-III device. For secure communication, the KSD-64A must be inserted into the STU-III device and activated through a connection process. The rugged, static-resistant nature of the KSD-64A makes it suitable for a wide range of office and industrial applications. [FMS90, p. 72]

S.   SUMMARY

AIT card technologies have been successfully implemented in many applications. This chapter provides a small sample of how AIT card technologies have been applied and some of the benefits the users of the systems have realized. Various research is being done in the DOD to implement these technologies in various applications, to include the DoD MARC card, the SRC card and the AMS card programs. As these AIT card technologies are researched for implementation, the personnel responsible for planning, designing, developing, testing, and implementing these systems must thoroughly understand the business process they are automating, address cost-benefit and life cycle management issues relating to the total system implementation and operation, address data management issues on the cards and in the card systems, to include how the data with be maintained and transmitted, and how security will be implemented in these card applications. By understanding the business process of the application that will be automated, and how it affects the overall business operation of the organization, questions and concerns about card program implementation can be addressed.

IV. DEVELOPMENT AND APPLICATION OF AIT CARD TECHNOLOGY MATRICES

Chapter II discusses the AIT resources used for AIT card systems. Chapter III identifies and discusses the applications of AIT card technologies. In this chapter, the information presented in Chapter II will be used as the basis to develop a functional capability matrix and the information presented in Chapter III will be used as the basis to develop a card application matrix. These matrices have been developed in a format to assist personnel in understanding and applying AIT card technologies. It should be noted that the matrices are tools which can be used to evaluate what card technology would best be suited for a specific application. The matrices can be use to generate ideas on where the AIT card technologies can be used for future applications.

A.   AIT CARD TECHNOLOGY FUNCTIONAL CAPABILITY MATRIX

In order to develop an AIT card functional capability matrix, identification of the various functional characteristics of each AIT resource must be established. Chapter II and Appendix A identify the AIT resources, their characteristics, and their strengths and weaknesses. Of these various characteristics that exist for the AIT resource, this author identified quantifiable and subjective characteristics to use as the basis for the development of the functional capability matrix. These functional characteristics are identified in Table 4. This list is not all inclusive of the various functional characteristics of the technologies, but is a representative sample of what functional characteristics should be considered in choosing an AIT resource to meet the user's need. The subjective characteristics are chosen based on the emphasis placed on these characteristics in the literature review, manufacturers' specification and related information, conference attendance, and communication with the experts in the area of AIT card technologies.

Applicability	Audit Trail Capability
Compatibility/Interoperability	Cost (Dollar Cost per Byte)
Data Storage Capability	Ease of Use
Electromagnetic Interference	Error Detection
Established Standards	Flexibility
Growth Potential/Expandability	Human Interaction for Operation
Information Security	Infrastructure Establishment
Interactive Operation	Line-of-Sight Operational Features
Logic/Decision Making Capability	Low/High Risk Technology
Open System Capability	Passive Operation
Proven Technology	Read/Write Device Contact
Security Features	Simple/Complex Technology
Survivability	Various Media
Vendor Support	

Table 4.   AIT Card Technologies Functional Characteristics

The definitions of the functionality characteristics used in the AIT Functional Capability Matrix are identified in Appendix B.

1. Development of the AIT Functional Capability Matrix

The matrix is developed in a format to assist the users in reviewing the AIT resource functional characteristics from a broad perspective or to identify a specific functional characteristic that will meet a user's unique concern. For example, in the broad perspective, the matrix can be used to identify (1) simple technologies to complex technologies, (2) earlier developed technologies to more recently developed technologies, (3) low data storage capacity to high data storage capacity, and (4) centralized (passive) to decentralized (interactive) database use. Figure 4.1 identifies the broad perspective functional capabilities viewpoint. This broad perspective can help the users begin to focus on what are
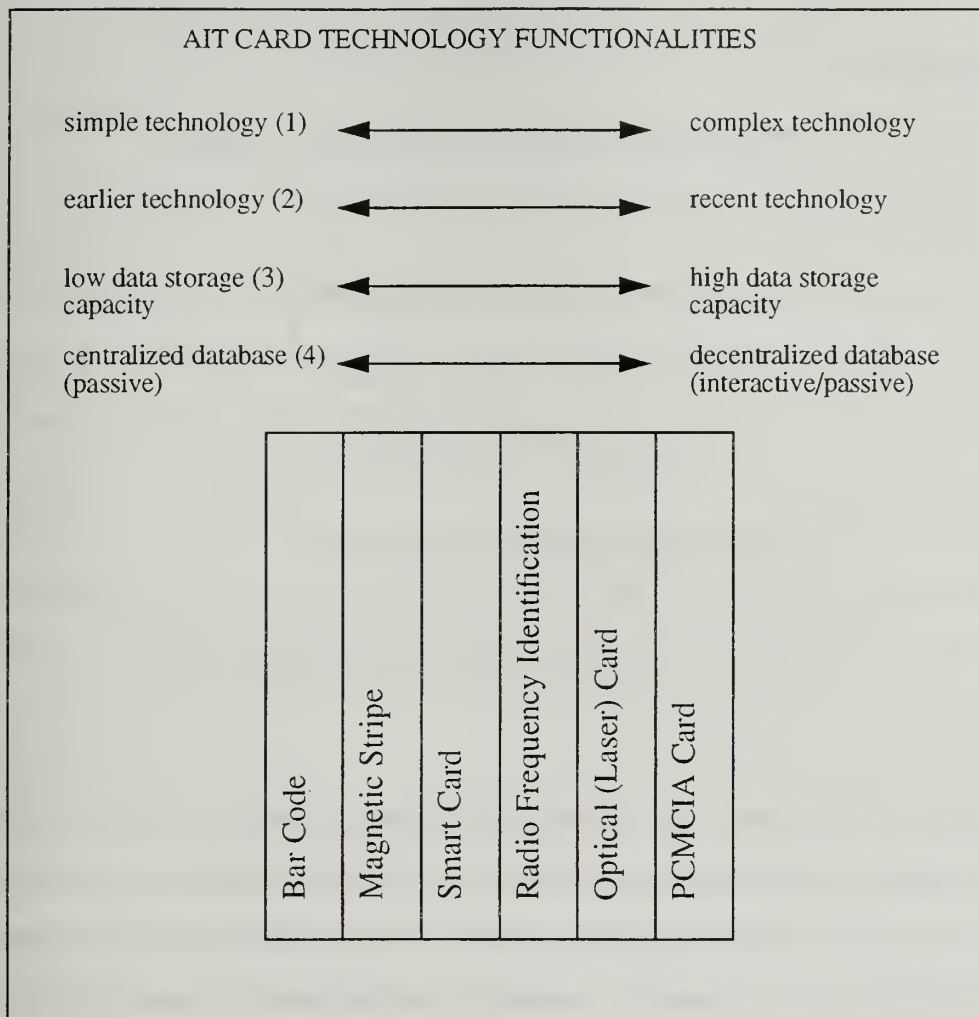
Figure 4.1: A Broad Perspective of AIT Card Technologies Functional Capabilities

the most important features of the application and the AIT resources which will meet their desired automation need. As the users become familiar with the technologies, the users can begin to focus on what are the specific issues they are interested in addressing with AIT resources.

Based on the information identified in Chapter II, the author chose to list the functional capabilities as the row attributes and the AIT resources as the column heading attributes. Both the row and the column can be expanded as new functional capabilities are

```
┌─────────────────────────────────────────────────┐
│         FUNCTIONAL CAPABILITY RATING SCALE        │
│                                                   │
│      (1) Capability/Desirability Rating Scale Diagram │
│           ┌───────────────────────────────┐       │
│           │      1        2        3       │       │
│           │                               │       │
│           │   ◄──┼────────┼────────┼──►    │       │
│           │                               │       │
│           │    Low    Average    High     │       │
│           │      Capability/Desirability   │       │
│           └───────────────────────────────┘       │
│                                                   │
│      (2) N = Not required, R = Required           │
└─────────────────────────────────────────────────┘
```
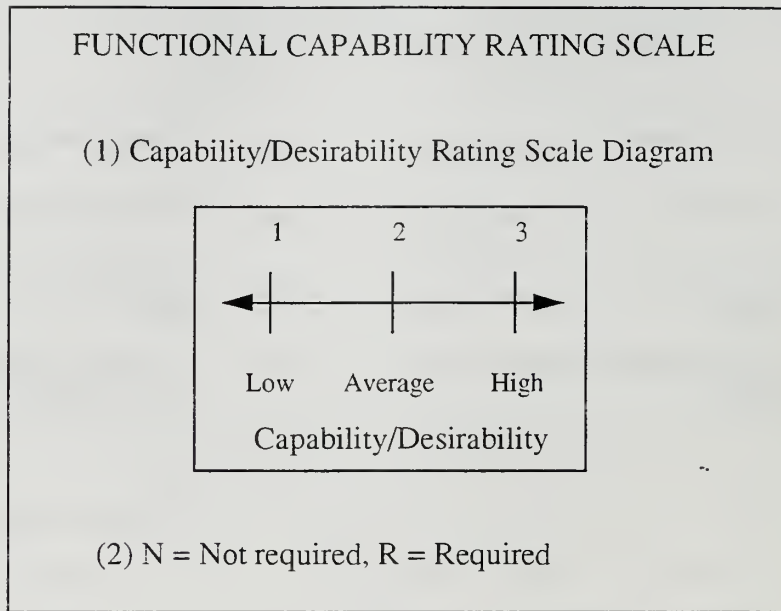
Figure 4.2: Functional Capability Rating Scale

considered (row attributes) and new technologies are identified (column attribute). The functional characteristic of the AIT resources identified in Table 4 were used in the development of the functional capability matrix. A Likert scale was developed and used as a descriptive rating scale to assign a capability and/or desirability rating for the specific AIT card technology characteristic. The Likert scale is identified in Figure 4.2. By viewing the matrix in this manner, users can focus their attention to the technology that can best meet their needs.

2. Application of the AIT Functional Capability Matrix

The following example is used to describe how the matrix can be used to identify a broad or a specific functional capability and/or desirable feature of the AIT resource. An example of a broad to a specific functional capability issue can be data storage capability of the various AIT card technologies. From the broad perspective, the user can view that a bar code is a low data storage AIT card technology medium, a smart card or RF/ID tag is

an average data storage AIT card technology medium, and a PCMCIA card is a high data storage AIT card technology medium.

From this broad perspective, the user can begin to address more specific issues of the AIT card technologies. Specific data storage capability characteristics exist for each of the AIT card media: A 1-D "linear" bar code symbology, like Code 39, can store up to 32 characters [MIL-STD-1189B, p. 13] and a 2-D bar code, like PDF 417, can store over 2KB [ITKI92]; the maximum data storage capability of the standard magnetic stripe is 150 characters (low density) or 475 characters (high density) [INFO94, p. 24]; the smart card data storage capability is up to 64KB [INFO94, p. 24]; a RF/ID tag data storage capability is up to 128KB [VOSS94, p. 390]; the optical card data storage capability is 6.6MB [OMDT93]; and the PCMCIA card data storage capability is 64MB. [HADD93, p. 389] Figure 4.3 identifies how the data storage capacity can be divided into sections: Section 1 would identify the AIT card technologies that have low data storage capacity between 0 and up to 1KB, Section 2 would identify the AIT card technologies that have medium data storage capacity between 1KB and less than 1MB, and Section 3 would identify the AIT card technologies that have high data storage capability greater than 1MB. Based on this information and the scale identified in the figure, bar code technology is assigned a rating of 2 (based on the symbology used), magnetic stripe technology is assigned a rating of 1, RF/ID and smart card technologies are assigned a rating of 2, and optical card and PCMCIA card technologies are assigned a rating of 3.

Based on the chosen quantifiable and subjective functional characteristics of the AIT card technologies listed in Table 4, a functional capability matrix is identified in Table 5. The rationale for the quantifiable and subjective evaluation values are identified in Appendix C.

When using these quantifiable and subjective characteristics in the AIT Functional Capability Matrix, the user must always keep in mind the application, use and purpose of the chosen media. For example, if the user is implementing a system with a centralized database and the card will operate passively, then the data storage characteristic might not be a major concern for the chosen AIT card media. On the other hand, if the user is
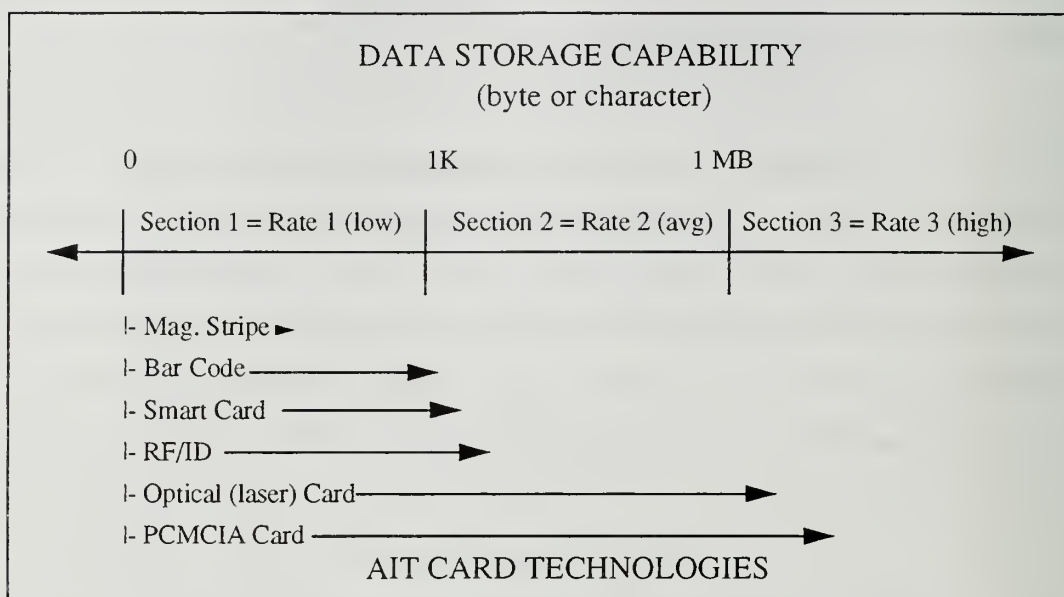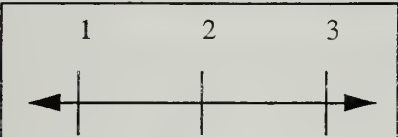
Figure 4.3: Data Storage Capability (by byte or character)
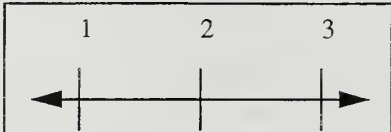
implementing a card system with a centralized or decentralized database and the card will be used for interactive and/or off-line operation, to store various amounts of data, then the data storage characteristic might be an important operational feature to consider. The AIT Functional Capability Matrix will benefit the user in identifying key functional attributes which can direct the users to the card media that will meet the established need. In addition, multiple AIT resources can be put on one card, a "Hybrid" card, to take advantage of the functional characteristics of each chosen AIT resource. Therefore, use of the AIT Functional Capability Matrix and the identified evaluation criteria are provided as a guide for implementation of the AIT card technologies. For specific applications, where the evaluation values do not pertain to the specific application, the evaluation value can be disregarded.

3. AIT Functional Capability Matrix Application Summary

The AIT Functional Capability Matrix is designed in a format to provide general information about the AIT card media and to make a general comparison of the AIT card media with reference to their various functional capabilities. The AIT Functional

Functional Capability Attributes N = Not Required R = Required Capability/Desirability	Bar Coding (A)	Magnetic stripe (B)	Smart Card (C)	RF/ID (D)	Optical Card (E)	PCMCIA Card (F)
Applicability (for various applications) (1)	3	3	3	3	3	3
Data Storage Capacity (2)	2	1	2	2	3	3
Ease of Use (3)	3	3	3	3	3	3
Electromagnetic Interference (EMI) (including permeance) (4)	3	1	1,2	3	3	1
Error Detection (transmission/reception) (5)	3		3	3	3	
Flexibility (for various applications) (6)	2	3	3	3	3	3
Growth Potential/Expandability (for various applications) (7)	3	3	3	3	3	3
Line of Sight Requirement (8)	R	R	R,N	R,N	R	R
Logic/Decision Making Capability (on the card) (9)	1	1	3	1	1	1
Mechanical Device Contact for Read/Write Operation (direct) (10)	3	1	1,3	3	3	1
No Human Intervention Required (11)	1,3	1	1,3	3	1,3	1
Open Systems Capability (12)	3	3	3	3	3	3
Operational Characteristic						
Interactive Operation (for decentralized database use) (13)	1	1	3	3	3	3
Passive Operation (for centralized database use) (14)	3	3	3	3	3	3
Proven Technology (15)	3	3	2	3	2	2
Security Features (physical, built-in) Available (16)	1	1	3	3	3	3
Audit Trail Capability (17)	1	1	3		3	
Information Security (resistance to duplication, counterfeit, tamper) (18)	1	1	3	3	3	3
Survivability (includes durability to various environmental conditions) (19)	1	1	1,2	3	3	2

Table 5: AIT Functional Capability Matrix

Functional Capability Attributes N = Not Required R = Required 1 2 3 ←——————→ Low Average High Capability/Desirability	Bar Coding (A)	Magnetic stripe (B)	Smart Card (C)	RF/ID (D)	Optical Card (E)	PCMCIA Card (F)
Technology issues						
Cost (Dollar/Byte or Character) [high cost (1) to low cost (3)] (20)	1,2	2	2	1,2	3	3
Infrastructure for Technology Well Established (21)	3	3	1	2	1	1
Simple Technology/Low Risk [high risk (1) to low risk (3)] (22)	3	3	2	2	2	2
Standards Established (ISO, ANSI, etc.) (23)	3	3	3	3	3	3
Other considerations						
Compatibility/Interoperability with Other Equipment (24)	3	3	2	3	2	2
Use of various media (plastic, cardboard, paper, etc.) (25)	3	3	1	3	1	1
Vendors (few (1) to many (3)) (26)	3	3	3	2	2	3

Table 5: AIT Functional Capability Matrix (Continued)

Note 1 (Column C): The double values assigned in the smart card column are used to identify contact and contactless smart card functional capabilities. The first number or letter identifies the rating for contact smart card technology and the second number or letter identifies the rating for contactless smart card technology. For example, the notation of cell 4-C in the matrix is 1,2, the notation of cell 8-C is R,N and the notation of cell 10-C in the matrix is 1,3. In this manner, the functional capability is identified in one cell for the AIT resource.

Note 2 (Row 11): The double values assigned for the human intervention criteria are based on the application of the AIT. Bar code technology is mainly used in operations that require a hand-held or stationary reader system operated by a human. Bar code technology can also be used in machine vision systems which does not require human intervention to read the bar code. [INTERMEC] Contactless smart card technology has been effectively used in toll road applications where a card is read as the car passes through an interrogator unit. [ATT93] Optical card technology has been effectively integrated with RF/ID technology. [CAPA94, p. 294]

Note 3 (Cell 20A): The double value is assigned to note the difference cost associated with the difference bar code symbologies, (e.g., 1-D and 2-D bar codes). The different symbologies have various data storage capabilities which will affect the calculated dollar/byte or character values.

Capability Matrix can assist a person who has a limited knowledge of AIT resources to the various characteristics and functional capabilities of the AIT card media. The AIT Functional Capability Matrix is not intended nor designed to provide the optimal solution to the user's problem(s) or concern (s), but to assist in the decision making process by providing information on what AIT card technologies are available, their key functional attributes, and the potential capability of the card technology to meet the identified needs.

The AIT Functional Capability Matrix is developed based on the author's knowledge and research of the subject matter. As these AIT card technologies evolve and change, new capabilities will arise. Therefore, the AIT Functional Capability Matrix can continue to grow and change. In addition to the information presented in the AIT Functionality Capability Matrix, specific details of the various card technologies can be obtained by contacting the various manufacturers and vendors of the specific AIT products.

B.   APPLICATION MATRIX

In order to develop an AIT card application matrix, identification of the various applications of each AIT resource must be undertaken. Chapter III identifies various applications of the AIT card technologies. The various applications identified in this chapter are a representative sample of the card technology application areas. Many card applications exist which can be used to further expand the AIT Card Application Matrix.

1. Development of the AIT Card Application Matrix

The AIT Card Application Matrix is developed in a format similar to the AIT Functional Capability Matrix. The application information identified in Chapter III is consolidated into a matrix format to assist a user focus on what applications have been designed and/or implemented with AIT card technologies. In this matrix, the row attribute identifies the application and the column attribute identifies the AIT card technology. Both the row and the column can be expanded as new applications are considered (row attribute) and new technologies are identified (column attribute). The enhancing technologies, biometric and voice data and machine vision, have been added to this matrix to identify those applications that use these technologies for additional functionality of the AIT card

system (i.e. access control, certification, authentication). The AIT Card Application Matrix is presented in Table 6. The reference information used to develop the application matrix is listed in Appendix D.

2. Application of the AIT Card Application Matrix

The AIT Card Application Matrix can be used in many fashions. The matrix can be used to (1) identify an application of interest to the user and assist them in choosing an AIT card technology, (2) identify the AIT card technologies used for various card system applications, and (3) identify applications that can support a "Hybrid" card technology implementation. The following three examples can assist a person in the use of the matrix.

Example 1: If the designer/developer is interested in the area of "Access Control" as an application, then the designer/developer can look at the application access control and find that bar code, magnetic stripe, RF/ID, smart card, and optical cards have been used for this application. In addition, biometric/voice data are also features to consider for card selection for this application. This is an example of how the matrix can be used to identify an application of interest to the user and assist them in the research effort leading to selection of an AIT card technology.

Example 2: If the designer/developer is interested in using a particular AIT card technology for various applications, then the designer/developer can identify which card technology supports the majority of the desired applications. For example, if the desired applications are access control, personnel identification, health service card, and debit/credit card, the AIT card technologies which have been applied in all four applications are magnetic stripe cards and smart cards. If an additional application is electronic certification, one solution could be the use of a smart card system. Therefore, by knowing that certain card technologies that have been applied in the particular application area, the designer/developer can focus their attention on the AIT resources which will meet the requirements for the desired application environment. This is an example of how the matrix can be used to identify the AIT card technologies used for various card system applications.

Applications	Bar Coding (A)	Magnetic Stripe (B)	Smart Card (C)	RF/ID (D)	Optical Card (E)	PCMCIA Card (F)	Biometric/Voice Data (G)	Machine Vision (H)
Access Control/Security (1)	X	X	X	X	X		X	
Campus Card (Student, Faculty, Support Personnel use) (2)	X	X	X				X	
Document Storage Card (large storage, software, documents) (3)					X	X		
Electronic Certification System (4)			X					
Electronic Ticketing (sports events, plays, theater, etc.) (5)		X	X				X	
Employee Card (Time, Attendance) (6)	X	X	X	X				
Financial								
Accounting System (Pay Disbursement, Fund Mgmt.) (7)	X	X	X					
Automated Teller Machine (ATM) (8)		X	X					
Credit Collection/Authorization Card (9)		X						
Electronic Benefits Transfer (EBT) (Public Asst. Program) (10)	X	X	X					
Prepaid Cash/POS/Debit/Cashless Card (ex. Vending) (11)	X	X	X					
Health Services								
Health Service Card (Patient Care/Monitor, Medicaid) (12)	X	X	X	X	X		X	
Insurance Card (13)		X	X					
Pharmacy Card (14)		X	X					
Library System (15)	X		X	X	X			
Logistics (Inventory/Material/Fuel Control; Mobility) (16)	X	X	X	X	X			
Manufacturing Operations (17)	X		X	X	X			X
Marketing Operations (Trade Shows, Conventions) (18)			X					
Personal Identification (19)	X	X	X	X	X		X	
Resource Management (Forestry, Licensing (Hunting), etc) (20)			X	X				
Retail Applications (retail/supermarket/valued customer) (21)	X	X	X	X	X			

Table 6: AIT Card Application Matrix

Applications	Bar Coding (A)	Magnetic Stripe (B)	Smart Card (C)	RF/ID (D)	Optical Card (E)	PCMCIA Card (F)	Biometric/Voice Data (G)	Machine Vision (H)
Services								
Farm Quota System/Agriculture (22)			X	X				
Job Training/Educational Service Card (23)			X					
Pay Telephone (24)		X	X		X			
Post Office System (processing, stamp purchases) (25)	X	X		X				X
School Lunch Card Program (26)		X						
Transportation								
Drivers License/Vehicle Registration/Vehicle Tracking (27)		X		X			X	
Electronic Toll Collection (ETC) and Traffic Control (28)	X	X	X	X				
Weigh Station Project (29)				X				
Other applications as products								
Modem/Fax (30)						X		
Network Interface Applications (31)			X			X		
Secure Telephone Unit (Smart Key) - Comm. Security (32)			X					

Table 6: AIT Card Application Matrix (Continued)

Example 3: If the designer/developer is interested in the best features of the AIT card technologies for various applications, the designer/developer may choose to use many AIT resources applied to one card, the "Hybrid" card. In this case, the designer/developer can use a combination approach from Example 1 and Example 2. This is an example of how the matrix can be used to identify applications that can support a "Hybrid" card technology implementation.

102

3. AIT Card Application Matrix Summary

By developing an AIT Card Application Matrix in this fashion, various trends can be observed which can be considered when identifying, evaluating and selecting an AIT card technology. The observed trends include:

- non-logic cards systems to intelligent, logic-capable card technology systems
- no or low security capability to more enhanced security capability of the card system
- small data storage capacity to large data storage capacity
- the movement from centralized database use to decentralized database use
- older technologies to the use of newer, more recently developed technologies
- the infrastructure, bar code and magnetic stripe technologies were used in many card applications

With the association of dates or time period to specific applications identified in the AIT Card Application Matrix, a tracking or forecasting approach can be established to identify the potential migration of AIT card technologies. For example, as a card application moves from a centralized database operation to a decentralized database operation, the AIT card technology may change and migrate from a magnetic stripe or bar code technology to smart card or another AIT card technology. Understanding the nature of the application environment is a key factor in the selection and acquisition strategy of an AIT card technology used to automate an application.

As information systems personnel and society become more aware of the available card technologies, and how they can and have been applied, the potential for future developments of card technologies and the identification of applications will continue to evolve and can have an effect on how every day business is conducted in the future. As noted from the development of this matrix, the established infrastructure of bar code and magnetic stripe card technologies have and will continue to have a definite place in the identification and selection of an AIT card technology for use in various applications. As the infrastructure is established for the other AIT card technologies, new application areas will continue to be identified.

C. SUMMARY

AIT card technologies can originate from a variety of sources using a variety of media and enhancing technologies. This chapter identifies the AIT card media technologies, their various functional capabilities, and the associated enhancing technologies that can be added to a card to enhance it functional capabilities. Matrices were developed to assist users of this technology identify the AIT resources that are appropriate to meet their needs. The AIT Functional Capability Matrix can be used as a tool to guide the users in the various functional characteristics of the technologies. The AIT Card Application Matrix can be used as a tool to guide the users in the various applications of the technologies. The AIT Card Application Matrix can be used as a guide to address future applications that could be adapted and used with the chosen technology.

The various technologies discussed were bar code, magnetic stripe, RF/ID, smart card, optical card, and PCMCIA cards.   The enhancing technologies discussed were biometric and voice data collection and machine vision. Each of these technologies have different operating characteristics, with various strength and weakness characteristics that must be consider for its use in various applications. For card applications, the card will be used in various environments, under various conditions, and for various purposes. The operating characteristics and the strengths and weaknesses of the various technologies must be considered when identifying, obtaining and implementing AIT for card application to obtain the desired AIT card system results.

Various technologies can be placed on a credit-size card and be used for various applications which arises from their functional capabilities. Some of these technologies have been in existence for many years, while some of the technologies have been recently developed. Continuous exploration of how these technologies can be used has resulted in the exploitation of their functional capabilities for various card technology applications. With an understanding of the technologies, their strengths and their weaknesses, and the identification of many areas of application, the opportunities for AIT card system applications are many for those who have the resources and the needs to implement these card technology systems.

V. CARD SYSTEM SECURITY

In a general sense, security is "the freedom from risk or danger" and covers a broad spectrum of areas. [RUSS91, p. 414] This chapter deals with card system security. Card system security can be divided into two security areas: physical security and information security. Physical security addresses security of the environment, card, equipment, and supplies. Information security addresses protection of the information. New and evolving card systems which automate applications can have potential system vulnerabilities that can weaken the card system. Therefore, mechanisms must be implemented to provide security to these systems.

A.   INTRODUCTION

Security is a key concern in many manual and automated systems and processes. In order to identify card system security concerns, an overview of the various security areas associated with these systems are identified:

- *Physical security of AIT resources* - protect the physical facility, the resources, and the card inventory,
- *Equipment security* - protect equipment and documentation from unauthorized use and theft, and ensure only authorized equipment can access the host computer,
- *Software and data security* - should reside in the terminals or the central processor to provide validation prior to authorization, message transmission, and protect against unauthorized access, use, and file modification,
- *Telecommunications security* - protect the system from the entry point to the completion of the transmission,
- *Personnel security* - addresses system and administrative user concerns,
- *Contingency planning* - permits restoration of the card system,
- *Emergency preparedness* - disaster planning, and
- *Other requirements* - ensure back-up procedures are in place for secure system access and monitor and audit to detect abuse at the transaction point.

[CASE93, pp. 807-808] [PFLE89, p. 459]

Security should be implemented on all systems, e.g., stand-alone, networked and distributed. Both stand-alone and distributed system operate without central host

interaction. Distributed system have special user concerns and problems. Proper data integrity measures must be implemented and only authorized users should have access to the data. A complete understanding of the application requirements and a thorough system analysis will facilitate the identification and design of security in the card system to address these concerns.

Authentication techniques should also be identified to reduce the system risks to comprise and/or failure. The current authentication methods include passwords, PINs, biometrics, challenge and response protocols and cryptography. Card system security measures help prevent unauthorized use, counterfeiting, and compromise of information on the card and in the host system. [NELS94, p. 47]

B.   INFORMATION SECURITY

Information security (INFOSEC) deals with the protection of information. The underlying roles of information security are to preserve the public trust and confidence that the information will be used only for its intended purpose, prevent fraudulent use, and preserve the legitimate interests of the owners and users of the information. [MURR94, p. 965] These information security roles are extremely important to protect information used to make decisions in our everyday lives. Therefore, it is critical that information be reliable and it be protected.

Information is all around us. There is information in newspapers, magazines, books, computer systems, and on cards (e.g., magnetic stripe card, IC cards). Information can be transmitted by various communication methods, e.g., telephone, television, and networks. Information in all of these systems is vulnerable to unauthorized access and compromise if the systems are not protected. These vulnerabilities can include tampering with authorization files, personal files, databases, interception of telecommunications, and card counterfeiting, as well as other vulnerabilities. [CASE93, p. 806] To ensure the information and the system are protected and secure, data integrity schemes, authentication methodologies, and cryptographic algorithms should be implemented.

C. DATA INTEGRITY

In order to provide information security to any system, the information and the systems should meet some minimum system requirements to ensure the data integrity is maintained. These minimum requirements should include:

- identify authorized users,
- use digital signatures and notary systems
- identify the simplest and smallest domain possible,
- keep processes simple,
- keep security functions separate from other functions,
- store secret information in stand-alone systems,
- transmit secret information only in secret codes,
- use parity checking and cryptographic checksums, and
- protect transmission channels.
[MURR94, p. 970] [PFLE89, pp. 396-399]

Each card system and its application will have various vulnerabilities. It is critical that the minimum system security requirements be identified and addressed to ensure the card system operate as required to meet the mission need.

D. AUTHENTICATION METHODS

One of the key components in any security environment is authentication of the user and the host system to which the user is requesting access. Authentication is the process of proving that a user and or the system is what it claims to be. There are various methods to verify the eligibility of a user or the system and grant access to certain information. [RUSS91, p. 399] The three basic methods to authenticate the user to the host system, and vice versa, are:

- what things are known (e.g., password, PIN)
- what objects are possessed (e.g., token, ticket, card)
- what characteristics are available (e.g. biometrics)
[PFLE89, p. 452]
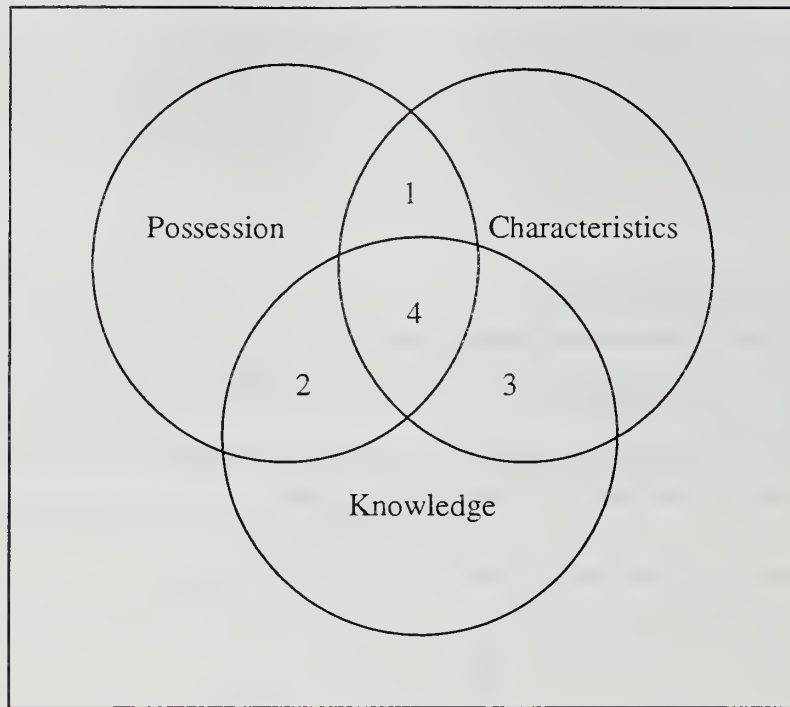
Figure 5.1: Basic Authentication Methods [MILL94, p. 194]

Figure 5.1 identifies the three methods and how they can be used. These basic methods can be used individually by the system or can be used in combination. An example of individual use is the possession of a ticket, which can be used to gain access to a system, such as a mass transit ticket. An example of possession and characteristics (Area 1) is an identification card with a photograph and/or some biometric information, like a thumbprint. An example of possession and knowledge (Area 2) is a credit card with a PIN number for access to an ATM system. An example of characteristics and knowledge (Area 3) is personnel recognition by a security guard at a institution. An example of possession, characteristics, and knowledge (Area 4) is a proximity badge or smart card that contains some physical features of the user (e.g., photograph) and requires a password or PIN to gain access to a limited access environment. Various combinations of these methods can be used for authentication of the user to the system. The system requirements should identify what

authentication method(s) are needed to provide the best solution for the particular application.

1. User Authentication

While some system application accept card possession as proof of an authorized user, other applications require the assurance that only the authorized user has access to the particular system. User authorization can be achieved by associating a specific user to a specific media, (e.g., a card) by some means, such as a password, a PIN, or by some biometric information. These systems can be challenge and response systems to ensure the card holder is the genuine owner of the card.

a. Password

A password is example of what things a person knows to gain access to a system. Passwords can be used with card systems. Passwords are made up of various alphanumeric characters (e.g., 1, 2, A, B, c, d) and special characters (e.g., %, @) and can be of various lengths. Passwords should be constructed with security in mind, vice something that is easy to remember, like a birth date or a name. The user enters the password string when queried by the authenticating device (e.g., a computer). The authenticating device verifies and authenticates the password to allow the identified user access the system.

This type of password is vulnerable to external sources and has many short comings. Passwords reveal their owners during each authentication attempt. They can be compromised; they are able to be guessed by various means (e.g. password cracker program, brute force); they are typically written somewhere; they are reused; and they are require by many systems to be changed in a certain time period. [WEBB93, p. 856-857] For some systems, password authentication is not adequate, especially where external callers remotely dial-in to networked system. [MUIR93, p. 900]

The one-time password, also known as dynamic password, method uses a smart card with processing capability and a battery. The smart card creates a different

password for each authentication attempt and synchronizes the passwords with the host system. The smart card and the host system generate new passwords for certain time periods and the host knows the token's current valid password at any given time. Therefore, the life time of each password can be short. The algorithm used for this process can be varied with each card and is kept secret. Dynamic password authentication are more secure than conventional password systems. Valid password are difficult to predict at any given time without knowing the initial value and the algorithm. These features of dynamic passwords ensure card authenticity. [NELS94, p. 49]

b. Personal Identification Number (PIN)

User authentication can be achieved by the specific user employing a personal identification number (PIN). The PIN is similar to a password, it is known only by the card holder. When the user keys the PIN into the system, the card or the system compares the PIN to a reference number stored in the host system. If the value matches the reference number, the user identity is verified and the user is allowed access to certain files identified in the system. A disadvantage of this authentication method is the PIN can be compromised. PINs are vulnerable to many of the same issues that plague passwords. Therefore, some systems encrypt the PIN before presentation to the card. An enciphered PIN system is most effective when the cryptographic key is valid for a single session [NELS94, p. 55], and is similar in function to a dynamic password.

c. Biometrics

Biometric authentication techniques use a person's biometric characteristics to authenticate the user to the system. The biometric traits can be physiological or behavioral characteristics of the user. Physiological characteristics include thumbprints, fingerprints, hand geometry, facial features, vein patterns, iris scan, and retina scan. Behavioral characteristics include signature dynamics, keystroke dynamics, and voice verification. [MILL94] These characteristics can not be forgotten and are extremely

difficult to forge which lead to successful user authentication in most cases. [PFLE89, pp. 453-454]

Choosing the right biometric system is essential to ensure the system will meet the security requirements needed in the application. The system should be evaluated by various factors to include the "level of confidence" the system can provide that the requestor is the authorized user, cost considerations, and user acceptance. The "level of confidence" can be consider in two manners: the "false acceptance rate (FAR)" which occurs when an unauthorized user is allowed access to the system or the "false rejection rate (FRR)" which occurs when an authorized user in not allowed access to the system. [MILL94, p.197] Costs of the different biometric systems vary based on the complexity of the systems. It is important to procure a system that will meet the authentication requirements of the application. Biometric systems can be intrusive to impose on the system users. Therefore, users should be aware of the needs for the specific biometric authentication system. Large security risk applications typically use biometric authentication. [NELS94, pp. 55, 58] In addition, data encryption programs can be used to protect biometric data from unauthorized use.

d. Challenge and Response

A challenge and response authentication system typically uses a smart token, therefore, it is considered a possession method of authentication. Most challenge and response systems use an integrated chip (IC) card to provide the logic capability for the challenge and response activity. The card should have a power source and memory capacity.

There are various types of challenge and response card system: a smart card, a super smart card, and a hand-held reader that senses dot patterns presented on a screen. The smart card's microprocessor can be preprogrammed for a specific calculation, i.e., the processor can be used to compute an encrypted form of some information to the card. The system obtains the encrypted information and processes it to authenticate the card. With the

111

super smart card, the user requests access the system, the system challenges the user, the user keys in the required information, the device computes the response, and the user inputs the displayed response to the system to gain access. The dot-sensing, hand-held reader requires interaction with the host and a display screen. The host computer system generates a random pattern of dots and displays the dot pattern to a screen. The user holds the reader to the screen to sense the dot pattern. The reader converts the dot pattern to a number and displays it to the user to key into the system to gain access. [PFLE89, p. 453] These smart cards and dot-readers can be used as an authentication device. The problem with these systems is, if the card is not possess by the owner, then unauthorized access can occur. Biometric information can be available on the card to identify the user is the authorized card holder.

2. Cryptographic Authentication

Cryptography is a means to secure data for various uses. Security of the data can be achieved by performing encryption and decryption functions to the data. Encryption is the process of taking plain text data and converting it to cypher text data by using one or more cryptographic keys. Decryption is the reverse process of encryption, which retrieves the plain text data. Many cryptographic algorithms exist today. Most cryptographic algorithms perform some advanced mathematical functions. Therefore, processing capability of the system is an important consideration in security system design and implementation. [MITG93, p. 71]

a. One-Way Encryption

One-way encryption uses one-way functions to encrypt the data. A one-way function is a mapping function that can map an instance of a simple element into a universe of another element. An simple example of a one-way function is $y = x^3$. One-way encryption is typically used for password authentication systems. In this case, x could represent the password and y is the resulting encrypted password. One-way encryption of passwords is typically effective against password attacks. [PFLE89, p. 160]

112

b. Symmetric Key Authentication

A symmetric key authentication system uses the same key system for the encryption and decryption process. Figure 5.2 is a simple example of a symmetric key authentication application. With these key systems, it is critical that each card should have a unique key. Therefore if the key is discovered, it does not compromise the entire system. The unique keying process should occur during the personalization of the card. [NELS94, p. 50] The following are symmetric key authentication algorithms used in many card systems.

(1)   The Data Encryption Standard (DES) algorithm is a "single key" encryption key and is classified as a symmetric key cryptography method commonly used with smart card systems. It uses a single key for both encryption and decryption. [MITG93, p. 72] The DES is owned by the government and is sanctioned by the National Institute of Standards and Technology (NIST). The DES algorithm is in the public domain for anyone to use. The secret cryptographic key is stored on the card and in the card acceptor device (CAD). [NELS94, p. 49] This encryption algorithm is used for securing government information systems up to the "Secret" classification level. [MITG93, p. 72]

(2)   Telepass 1 is a one-way algorithm used with smart card systems. This algorithm uses a secret key, the contents of a specific word in the card's memory, and a random external value to compute the response to the challenge in the challenge and response authentication process. [NELS94, p. 50]

$$
\begin{aligned}
k &= \text{key} \\
x &= \text{plain text} = D\,(y_k) \\
y &= \text{cipher text} = E\,(x_k)
\end{aligned}
$$

Figure 5.2: Example of Symmetric Key Application

c. Asymmetric Key Authentication

The asymmetric key authentication system uses two cryptographic keys in the authentication process. Smart card systems are typically the card system of choice for asymmetric key authentication systems. Each key set consists of two keys which can be use in a public and private manner. The public key is available in the public domain, in an electronic directory, and the private key is kept secret. The CAD has a public key and a private key, with the public key typically used by the CAD in the authentication process. The smart card has a public key and a private key, with the private key typically used in the authentication process. The smart card's private key can be used to generate an electronic signature and the CAD's public key can be used to authenticate the signature. [NELS94, p. 51] The cards used with these algorithms typically required computational capabilities and large memory storage capacity. [MITG93, p. 72]

(1) Public-Private Key Cryptography is an asymmetric key authentication method that uses a unique related pair of keys. Either key in the pair may be used the encrypt the data, and the other key in the pair is used to decrypt the data. The private key remains in the possession of the key pair owner and the public key is made public knowledge through an electronic public key certificate. The public key certificate is used to verify the owner of the public key. This key cryptography can generate non-reputable electronic signatures to verify the integrity of the signed data, and non-reputable electronic receipts. It is a highly reliable method for authentication of users, entities, and applications of the system. It provides secure logon access for single, networked, and distributed computer system. These systems maintain the privacy, confidentiality, integrity, and certification of the data, the software, and the electronic documents. It is a method used for electronic commerce (electronic data interchange - EDI), electronic balloting, and privacy enhanced electronic mail. It can be used for electronic signatures and trusted date/time stamping of electronic documents, electronic mail, data, and software. And through this authentication method, a signed audit trail can be maintained of all uses

of each card. Therefore, this cryptographic key authentication method can be successfully used in many application environments. [SHOM94]

(2) The Digital Signature Standard (DSS) is an asymmetric key authentication method that was developed by NIST for generating document signatures in the United States Government. A digital signature is an electronic signature, similar is function to a handwritten signature. This digital signature is an encrypted string of data representing a pseudo signature with a time and date stamp and a condensed (hash) form of the document, which allows electronic tagging of a document. If the document changes, the hash changes. [MITG93, p. 74] This is a valuable feature to have for repudiation, verification, and authentication of the transmitted information. The DSS has been used with smart card technology for authentication purposes. One of the main strengths of the DSS algorithm results from the difficulty in computing discrete algorithms. [NELS94, p. 51] Digital signatures are used to proved authenticity of various documents. Equipment with smart card interfaces, such as telephones, modems, fax machines, and wireless broadcast equipment will be able to communicate in total security with the use of digital signatures. [MITG93, p. 74]

(3) The Rivest-Shamir-Adelman (RSA) algorithm is an asymmetric key authentication method developed and introduced in 1978. The name of this algorithm was derived from its three inventors, Rivest, Shamir, and Aledman. [PFLE89, p. 100] The underlying basis of this cryptographic algorithm is in the difficulty of factoring large prime numbers. Use of RSA as a cryptographic authentication method requires a microprocessor that can perform exponentiation for computing the electronic signature, a relatively large RAM capacity for storing intermediate values, large program memory for storing the instructions of the algorithm, and computing time. Smart cards used for the RSA algorithm typically cost more than general purpose smart cards. [NELS94, p. 51]

d. Kerberos

Kerberos is a trusted third-party encryption-based authentication service that can be used to identify and verify users requesting service on unsecure, untrusted networks, including distributed networks. Kerberos can authenticate the client and the server of the network. Kerberos uses an encryption key to gain access to the network vice having a password. The encryption keys, also know as session keys, are exchanged between each client and server for authentication. The encryption key can be used by the application for integrity checks. The key is never sent across the network, but possession of the key is demonstrated by encrypting a nonce[1], [WEBB93, pp. 855, 859-862] sometimes referred to as a ticket. The ticket is sent through the network to the designated locations. [STEM93]

Kerberos has many network security features. Integrity and privacy of the user request and the response are achieved. The system is protected against eavesdropping, malicious servers, and network attacks. Recent versions of Kerberos (e.g., Kerberos 5.0) uses a token to support authentication and authorization of the user. Smart cards have been used as the token in Kerberos applications. [WEBB93, pp. 861, 866-867]

e. Cryptographic Authentication Summary

Cryptography is an effective way to secure data without revealing the identifying characteristics or keys of the system to external sources. Cryptologic authentication methods require key distribution. Key management can be a vulnerability with systems using cryptographic methods. The key management process increases the system complexity, adds system administration overhead, and reduces the flexibility of the system. [NELS94, pp. 48, 52-53] Therefore, the security plan should address key management issues if this method of authentication is used.

---

[1] A nonce is a word invented or used for a particular occasion. [WEBS88, p. 798]

3. Zero-Knowledge Authentication

A. Fiat and A. Shamir developed the first practical zero-knowledge protocol authentication approach. Zero-knowledge authentication is a challenge and response method using smart card technology. Zero-knowledge protocols require the use of smart cards to provide the authentication of the accreditation values assigned to the card. The authentication technique requires the card issuer to compute a public system constant from the product of two large prime numbers. Each card is assigned an identification word. Each card is loaded with the set of (k) secret accreditation values formed using a hash function with the card identification word. In the challenge and response authentication process, the verifier issues one or more challenges and the prover responds with an equal number of responses. Throughout this challenge and response process, the secret accreditation values are never revealed which enhances system security. [NELS94, p. 52]

Zero-knowledge protocols can be a viable authentication method to use for card system security. Zero-knowledge protocols are less vulnerable to key compromise than cryptographic authentication methods since they do not use passwords or cryptographic keys. These protocols require sophisticated microprocessor smart cards with random number generators and exponentiation units. They also require the smart card be initialized in a single location, with the assigned secret accreditation values remaining in the card. A benefit of using these protocols is the security level of this technique increases exponentially with an increase in the number of challenge/response pairs and the number of accreditation values. However, increasing the number of transactions and accreditation values increases the processing time and memory requirements. The need for sophisticated microprocessors and the reduced usable memory increases the overall smart card cost. However, zero-knowledge protocol require no key management overhead which can reduce the overall system cost. [NELS94, pp. 53, 55]

E. HOLOGRAPHIC SEALS

A holographic seal, known as a hologram, is a unique photographic printing from a laser light source on the surface of a card that gives it a three dimensional effect. To a viewer, the hologram provides information about the shape, contour and position of the all the objects recorded in it. [WIHO94] The hologram can be used for card security or for an aesthetic effect. For card security, the holograms is an attempt to reduce fraudulent duplication and deter counterfeiting of the card. Even with the hologram applied to the card, the card must still be viewed by the authenticating/authorizing personnel to correctly identify the user. Holographic technology has been applied in various areas to include advertising, publishing, security, anti-counterfeiting applications, product design, [HOLO94] and manufacturing. [WIHO94]

F. SECURITY SYSTEM SELECTION

The selection of the "best" authentication method comes from a thorough system and risk analysis. The system and risk analysis should cover the following:

- Identify the assets,
- Identify all known and potential system vulnerabilities,
- Estimate the likelihood and potential magnitude of exploitation (modification, denial of service, loss or destruction) of each vulnerability,
- Using cost-benefit analysis, assess the effectiveness of the current prevention and detection strategies and compute expected loss,
- Assess applicable prevention and detection security controls and their costs, and
- Implement security measures and guidelines to manage the system security throughout the system life cycle (e.g., design, development, implementation, and operation).

[CASE93, pp. 808] [PFLE89, pp. 458]

A thorough system and risk analysis should result in identifying the appropriate technology selection for meeting the application requirements. The analysis should address the cost and benefits of each identified alternative solution. The trade-offs between costs, efficiencies, system security requirements, and end-user ease must meet the

application requirements and the customer demands. The user authentication method depends on the application requirements, from no user authentication to positive user authentication. The selected security method should address the identified vulnerabilities, including the compromise of passwords, PIN, and cryptographic keys. [NELS94, pp. 56-57] In addition, the card should be design as a sealed token with no input requirement, if possible. With this design feature, the card can be rendered inoperable if the seal is broken. [PFLE89, pp. 453]

Network security issues should address various areas. They should address system reliability, access (dedicated and dial-up), and capacity issues. Networks should be flexible, sensitive, and support the end-user. User ID, password and PIN security are not totally adequate in these systems, especially for remote access. Biometrics and/or voice recognition systems also have their limitations. Biometrics can be intrusive to system users and voice recognition systems can be expensive. Token technology is available, easy to use and administer, seems to be very reliable, and it can provides an additional layer of security over password security. [MUIR93, p. 900] Figure 5.3 is an example of a card to host system network operation.
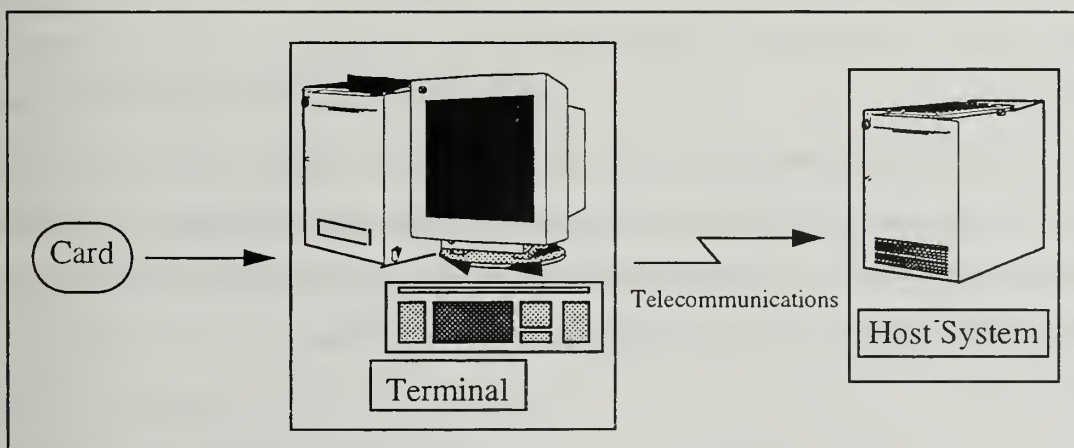
Figure 5.3: Card to Host System Operation [CASE93, pp. 809]

G. SUMMARY

In summary, card system security is an extremely important consideration is any card system. Based on the thorough system analysis of the application environment, an accurate evaluation of the mission requirements including the necessary security requirements, one can begin to identify what security mechanisms are available to establish a adequate security program to protect the information in the card system and the application environment.

Many authentication methods are available to meet the various security requirements of the card system and the application. Users and other entities must be authenticated to obtain access to the system. User authentication can be accomplished by passwords, PINs, biometric characteristics, challenge and response and cryptography. These system can be designed to be challenge and response driven to ensure the card holder is the genuine owner of the card. Each of these methods has advantages and limitations which must be assessed to ensure security requirements of the application are being met. The card used in the application can be designed with holographic seals to protect the card material from alteration and fraudulent use.

The selection of the card security system that best meets the mission need is one of the most important considerations in any card system. The factors that drive this selection include identifying the security requirements, identifying the assets available to address these security requirements, identify the information and system vulnerabilities and the likelihood of occurrence. Once this is completed, a cost-benefit analysis of the available systems should be accomplished to identify an adequate system and alternative systems. Security measures and guidelines for managing system security throughout the life cycle should be established and implemented. The end-users of the system play a key role in system security and must be key players in this environment.

VI. AIT SYSTEM SELECTION AND ACQUISITION METHODOLOGY

DoD has many initiatives underway to address the present acquisition process of ADP resources, which include AIT resources. The focus of these initiatives are performance-based specifications based on key mission essential needs which are identified by their functional and sub-functional requirements. The present acquisition process come under the business improvement concept to minimize redundant data entry and increase documentation speed, processing, and quality throughout the automated systems. The information for these systems comes from various resources, to include demographic, readiness, and logistics information, to list a few. The potential savings of these automated systems are realized in time, money, personnel and material processing, asset tracking, and visibility, which yield many returns on investment, in tangible and intangible terms. Real time information transmissions can be obtained with these automated systems, which facilitates critical decision-making for strategic operations. A key component in this real-time information transmission is ensuring the right assets are in the right place at the right time. Acquiring the assets to meet these needs is critical and this is why AIT resource selection and acquisition should be done in a proper manner with a well thought out acquisition methodology to guide personnel making these resource decisions.

A.   ACQUISITION POLICY VISION

The overall acquisition vision is to procure resources using performance-based specifications, nongovernment standards, and commercial item descriptions (CIDs). Unique military specifications and standards should only be used when requirements can not be met in any other manner. [RPAT94, p. 3] There are several key elements in the acquisition agenda, which includes adoption of commercial practices, partnering with industry, activity-based costing (ABC), and integrated product development (IPD). [RPAT94, pp. 7-10]

- *Commercial practices* involves the development of procedures that resemble commercial procurement practices for acquiring systems and resources.

- *Partnering with industry* involves the use of performance-based specifications and reduced program oversight to improve the working relationships with industry.

- *Activity-Based Costing (ABC)* is used to generate a direct correlation between costs and activities/processes by specific requirements. Contractors should be encouraged to establish and use ABC and activity-based management.

- *Integrated Product Development (IPD)* is a risk management tool used with performance-based specifications. It addresses key issues in development, engineering, and production.

The DoD acquisition and procurement goal is to use performance and commercial specifications and standards. Performance-based specifications are used to define "what is needed" in terms of performance and interface requirement of the item or system. With performance-based specifications, the focus is how the item or system performs with the larger system and not how the product is design and manufactured. [RPAT94, p. 18] By using performance-based specifications, DoD can procure resources from the commercial marketplace to meet mission requirements. [PERR94] Through commercial-of-the-shelf (COTS) procurement, the industry specification and standards can be infused into DoD and other government services. New systems should be described in performance-based specifications to maximize the use of COTS and generate avenues where manufacturers can offer various design and manufacturing experience. [RPAT94, p. 11] [PERR94]

Another initiative in the DoD vision is the Corporate Information Management (CIM) initiative. The CIM initiative for acquisition is being mandated to address the need to communicate electronically among government and industry. [RPAT94, p. 6] The overall goal of the CIM initiative is to standardize DoD processes using business process improvement techniques to identify functional needs and to procure the technology that can best resolve those needs. The CIM offices should address specifications and standards preparation and how they will be used in the acquisition process. The CIM concept is portrayed in Figure 6.1. [TMIS94, p. 9]

CIM CONCEPT
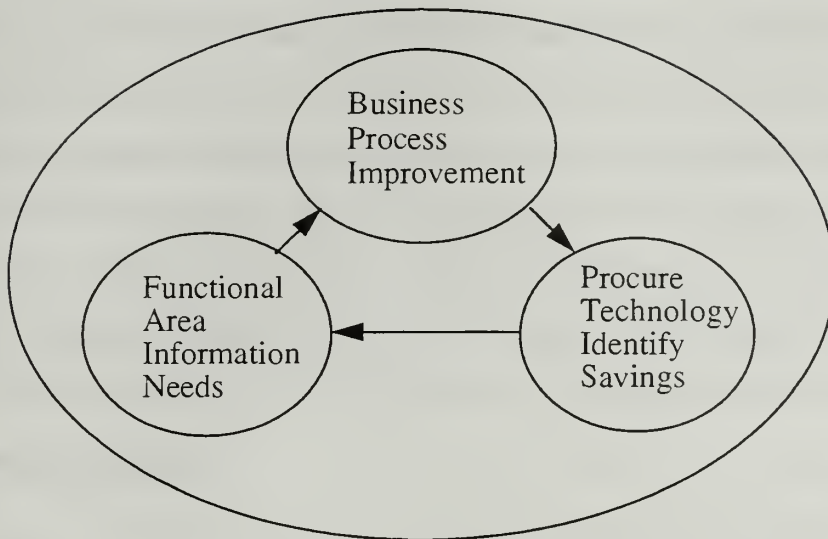
Figure 6.1: CIM Concept [TMIS94, p. 9]

By understanding the various initiatives that have been proposed for use in the acquisition process, the remaining challenging issue that must be addressed is effectively identifying the requirements and the resources that will meet the mission need. The problem does not begin with identifying the appropriate standards to use, but ensuring cost-performance trade-off and various analyses adequately justify meeting the specific system requirements (functional, technical). This begins in the requirement development phase of the acquisition cycle. Some technology tools that are being promoted for use in DoD in this area, include Distributed Interactive Simulation (DIS), Design to Cost, and Cooperative Research and Development Agreements to perform cost/performance trade-offs and dual use capability analysis. [RPAT94, p. 7]

The DoD acquisition process is undergoing numerous changes and education is key to effectively promoting the change and to develop acquisition methodologies and strategies in line with these changes. The four fundamental areas to address in this process are training, leadership, management, and funding. Training provides new skills and knowledge. This is key to implementing any acquisition strategy. The acquisition work force must be trained in the tools and techniques of risk management vice risk avoidance

in the acquisition process. Leadership entails both visibility and strategic planning. Leaders must be involved in the acquisition change process since this will ultimately affect how resources will be acquired by their subordinate personnel. A strategic plan, a vision of "where to be" and "how to get there" with concrete direction, milestones, and metrics must be developed. The highest level in the organizations charged with implementing the plan should be an integral part in the strategy formulation. Management implies authority, and personnel with this authority and responsibility should have the DoD corporate or service strategic plan in mind. These management personnel should have some control over the process and over the funding allocations to implement the activities to achieve the strategic vision. Funding is the ultimate stumbling block and the leadership must ensure that adequate funding levels are met in critical areas. [RPAT94, pp. 7-9]

With the DoD's declining procurement budgets and the new acquisition policy, DoD personnel should be encouraged to use performance-based standards, COTS, process control management, and nongovernment standards (NGS) in the design, development, and acquisition of resources. The overall goal should be to reduce program oversight; manage risk; quantify costs and savings through cost-performance analyses; and design, develop and implement flexible systems to meet various mission needs. [RPAT94, p. 5] In addition to these acquisition policy issues, the acquisition process should address the infrastructure of the organization, technology infrastructure in industry, and interoperability and open system compatibility issues that can affect the overall integration and operation of the system.

With this in mind, and the increasing use of AIT resources to meet mission critical needs, in such areas as In-Transit Visibility (ITV), Total-Asset Visibility (TAV), Theater Medical Information System (TMIS), and various other systems, the following acquisition methodology can be used as a guideline to focus personnel in AIT resource procurement. [DEPT94] The acquisition strategy should identify the system that will meet the present needs and address a migration path to the future technologies that might be implemented at the end of the present system's useful service life.

B.   ACQUISITION METHODOLOGY

The acquisition methodology[1] should cover the total acquisition process, from identifying viable requirements that must be addressed to meet a specific mission need through the life cycle management of the implemented system. The acquisition goal is to implement the system that matches your present application requirement(s) and address the migration of the system to meet potential future requirement(s). The following acquisition methodology can be used to identify and meet the present and future mission need. Table 7 identifies the major system components to be consider in an AIT system acquisition.

1. Definition Phase

The Definition Phase should include the identification and formation of a project team who will be responsible for total acquisition of the system from the mission needs analysis and assessment to the implementation of the AIT system. The project team should define the problem, establish the scope for resolving the problem, and assess the feasibility to resolve the problem with the available technology.

2. Requirements Phase

The requirement phase consists of conducting a requirement analysis of the system which is to be automated and the identification of the system functional requirements to meet the mission need. Performance specifications should be developed to meet the identified functional and sub-functional requirements. The present DoD policy is "Every DoD requirement should be justified and well-defined, and DoD specifications should not have non-value-added requirements." [RPAT, p. 3]

---

[1] The acquisition methodology was developed from the author's knowledge of the subject matter, reference information identified in the text, Figure 4.5: A Systems Development Life Cycle [WHIT89], and Figure 3.2: Summary of Database and Application Development [KROE92].

Hardware	Software
- IBM PC or Compatible Computer (486 configuration or better preferred)	- DOS
	- Application Software Modules
- Card Reader/Writer System	- Reader/Writer Drivers
- Printer (laser printer preferred)	- Printer Drivers
- Scanner System (e.g., bar code, optical)	- Scanner Software (when required)
- Interrogator System (e.g., RF/ID, contactless technologies)	- System Design/Integration Requirements (including performance, schedules, and costs)
- Cards/tags	
- Interface Equipment (e.g., biometric systems)	
- Telecommunication Accessories (e.g., modem)	
- Other Accessories (e.g., additional cables)	

Input	Output
- Data Sources	- Database System
- System Operating and Maintenance Issues	- Printer Reports
- Training	
- Facility Requirement (environment, electrical)	

Table 7. AIT System Components

In the requirement phase, a mission requirement analysis, functional analysis and allocation assessment should be conducted. The mission requirement analysis should identify the mission objectives, impact of the system's operational characteristics including the present life cycle management process, present threat(s) and risk(s), environmental issues, minimum acceptable functional and subfunctional requirements, and the technical performance of the system to include telecommunication requirements. The analysis should examine the present system for validity, consistency, desirability, and attainability with respect to current resources (e.g., skilled personnel, equipment, facilities), present

technology, life cycle management costs, and any other constraints which will affect the mission. The results of the analysis should verify the existing requirements or lead to the development of new requirements which meet the mission. [MIL-STD-499A, p. 15]

The functional analysis should identify and analyze system functions and sub-functions which meet system performance and design requirements. Performance requirements shall be established for each identified function and sub-function. The functions and sub-functions should be reviewed periodically for validity and verification to meet the system performance and design requirement. [MIL-STD-499A, p. 15]

The allocation assessment is designed for each valid function and sub-function to have associated performance and design requirements for the total mission requirements to be met. The mission requirements shall be stated in detail for the proper allocation of resources (e.g., hardware, computer support, personnel, data, and facilities). Special skills or requirements should be identified. Allocated requirements shall be traceable to the system functional requirements they are designed to address. [MIL-STD-499A, p. 15]

Trade-off studies should be conducted, when appropriate. The trade-off studies can consist of time-line analysis, system design synthesis, and system/cost effectiveness analysis. Trade-off studies shall be accomplished at various levels of functional or system detail. [MIL-STD-499A, p. 17]

Once the functional and subfunctional requirements are identified, the present funding should be assessed and user models should be created. The users should be interviewed to ensure all the user requirements have been identified. Prototypes or similar developed programs can be used to assess user requirements to facilitate automation of the specific mission need or process.

3. Planning Phase

The Planning Phase consists of planning the system that will meet the present mission requirements and establishing a migration plan for the present system to meet future projected needs. Within the planning phase, a review of the available AIT systems

and the various capabilities and costs associated with each AIT systems must be researched. The planning phase should include the following actions:

- Identify AIT system(s) to meet the current mission need(s)
- Identify AIT system(s) to meet the future mission need(s)
- Configuration management
- Communication with expert personnel

By addressing the issues identified in these action areas and communicating with the experts on the desired AIT system plan, the system developer will have a thorough understanding of the system they are automating to meet an identified mission need. A proof of concepts can be initiated in this phase.

a. Identify AIT System to Meet Current Mission Need(s)

Identify the AIT system(s) that will meet the current application requirements with the available funding. This includes the identification of the present user base (e.g., 1000 people), the functional/technical aspects of the any present AIT systems, the number of card and card system equipment at each activity and their associated costs, the media (e.g., type, size, shape, location) [TMIS, p. 17], research and development costs, system integration and production costs, total system operation and maintenance costs (e.g., life cycle management costs), training costs, facilities cost to include electronic circuitry and telecommunication resources, and any risk management issues and their associated costs. Risk management deals with the identification of system risks, to include security concerns, electrical requirement and resources, disaster planning, backup and recovery procedures, potential for the use of obsolete technology, and other related risk management issues.

b. Identify AIT System to Meet Future Mission Need(s)

Identify and forecast what and where the automated activity should be in the future (e.g., next 5 to 10 years). This activity includes identification of the AIT system (s)

that will meet the projected future needs and establish a migration plan to get from the current application to the future application environment. [TMIS94, p. 17] This plan should include the future user base (e.g., 1000 people to 100,000 people), the projected number of cards and card system equipment at each activity and their projected associated costs, life cycle management costs, risk management, and any additional costs associated with the future migration plan. This plan should include the identification and review of alternative AIT resources to support automated identification technology improvements.

c. Configuration Management

Configuration management is based on decisions made in the system engineering process which includes the automation of a system throughout its life cycle. As defined in DoD Instruction 5000.2, a "configuration item" is "an aggregation of hardware or software that satisfies an end use function and is designated by the government for separate configuration management. Computer hardware and software will be treated as configuration items. Computer software will be treated as computer software configuration items throughout the life of the program regardless of how the software will be stored (e.g., read-only memory devices, magnetic tape or disc, compact discs, nonvolatile random access memory). Configuration management activities should be conducted in the system acquisition process." [DODI 5000.2] Configuration management should be done early in the acquisition process so configuration management issues can be identified and addressed as they occur. Therefore, configuration management should begin in the planning phase and continue in the follow-on phases. Configuration management includes:

- identify, verify, and document functional/physical characteristics of the AIT system,
- control changes to the AIT system and its documentation,
- record the configuration of AIT system, and
- audit the AIT system to ensure it meets the stated performance specifications

Configuration management should be applied to any AIT system, including systems with the development of technical data to support commercial-off-the-shelf (COTS) equipment, software, and their system integration. Telecommunication and any system integration costs should be assess and included in all planning documents. These costs can become exceeding high and must be monitored to ensure the right configuration is being planned, designed and implemented in card system. Any configuration changes that will impact proposed changes to functional and physical characteristics will be evaluated, and when approved, all documentation (e.g., specifications, programmer manuals, operator manuals, training material, maintenance data) will be updated to reflect the approved design changes and made available with the implementation of the change. All configuration changes will be bundled together in a program "change kit" and tested to ensure the change kit is adequate and complete before distribution. [DODI 5000.2]

d. Communication with Expert Personnel

In the planning phase, communication with expert personnel, in industry and in the government service, is key to identifying present AIT systems already in place and obtain feedback on the AIT systems and their integration from a practical experience point of view. Various companies in the AIT industry participate in national conferences where personnel can acquire AIT resource information. The government service has various AIT program offices and expert personnel who work with AIT resources and MITLA projects. By communicating with these expert personnel, valuable information can be obtained to address any concerns or issues might surface that could have been overlooked in the planning process.

4. Evaluation Phase

The Evaluation Phase should consist of the selection of the AIT system architecture, reassessment of the identified mission requirement and reassessment of the feasibility of the chosen AIT to meet the identified mission requirement(s). Use of Functional Economic Analysis (FEA), function point assessment, cost-benefit analysis or any other methodology

can be beneficial in identifying a feasible AIT system. The economic analysis should address system integration costs and the costs associated with fielding the total AIT system (e.g., card/tag, equipment, facilities, electrical requirements). In addition, a key element in the selection process should be to match the application requirements to the features of the available technologies. Some key criteria to use in evaluating the technology to the application are ergonomics, ease of use, data storage capacity, interactive or passive system operation, high or low throughput requirement, speed of transaction, retrieval efficiency, and the general standard considerations of cost, additional operational features, and card system reliability. Workplace considerations, such as hot or cold, wet or dry, dirty and hazardous environments should be assessed and can affect the AIT card system selection process for certain applications and/or may require containerization of the card. [MOOR94]

Selecting a card system and its associated equipment involves review of the application and review of the AIT card technology and it's various characteristics, an analysis of the reader/writer features and it's ability to meet the application requirements, and trying the equipment in the actual application or similar application (if the application is being developed) for which it is being selected. Communication with other people who have used the type of card system being selected will influence the decision making and selection process. The critical question to ask in the selection process should be "Does the card system best meet the application requirements?" This question should address present and future planning issues. If the card system characteristics do not meet the application requirements, then the result could be a card system that is inadequate, it does not meet the application requirements, or a card system that costs too much and might not be effectively used to its full potential. [MOOR94]

5. Design Phase

The design of the AIT card system will be completed in the Design Phase. The basic AIT card system application design should address the following issues:

- What application is being automated?
- What are the current features of the application that "need" to be automated?
- How will the card and the card system be used?
- When will the card and the card system be used?
- Where will the card and the card system be used?
- What will the card and the card system be used for?

In the design of the AIT card system, the design should include all necessary application requirements that are mission essential, as a minimum. The bulletized items listed above should be addressed. The designer should also consider how the card system will be integrated in the organizational processes and determine if any processes should be re-engineered to best use the AIT card system to its fullest potential. The designer should address the card use in centralized database system or decentralized database systems. In this process, the designer should address menus, forms, query and reporting facilities with the host system and the card and the card system interface; specify update, display, and control mechanisms of the card and card systems; and address any design program logic requirement in the card and card system. This can include the use of biometric and voice recognition system interfaces, for example. Additional issues that should be addresses in the design phase are the acceptance and compatibility of the human performance requirements, to include personnel selection to operate and use the card system, training, and other man-machine interfaces issues to integrated humans with the card system. [MIL-STD-499A]

In the area of configuration control, if government personnel design the system, then the responsible organization should have documentation to identify, document, and verify the functional and physical characteristics of the AIT card system, control any changes to the AIT card system and its documentation, record the configuration of AIT system, and audit the AIT system to ensure it meets the stated performance specifications. [DODI 5000.2] Process controls and non-government standards should be used in the design process. If the design is to be completed by contractors, the current policy is the government should only maintain configuration control of the functional and performance

requirements, with the contractors responsible for the system design. [PERR94, p. 4] [RPAT94, pp. 2-5]

6. Test the System

The AIT card system will be tested to ensure it meets the identified system requirements, interface criteria, and performance-based specifications. The test results should be evaluated and deficiencies corrected to ensure the system operates as required. Various technical and cost analyses should be completed to ensure the system is ready for implementation.

7. Implement the System

The AIT system will be constructed to meet the mission essential application requirements. The AIT system and the applications can be installed at the activities that meet the identified mission requirements.

8. Review System Operation and Risk Management

The AIT system operation should be continually reviewed to ensure its meets the stated mission requirements. The review of the AIT system should include a continuing analysis of the risks associated with the system cost, its functional capability, and the technical features of the AIT system. The analysis should identify any critical areas that should be further investigated for potential problems and address how to resolve the identified problems and/or establish corrective action. [MIL-STD-499A, p. 11]

9. Maintain the System: Life Cycle Management (LCM)

The maintenance of the system will be an iterative process to ensure it functions properly and continues to meet the mission need. Each AIT system has various system components which have different replacement considerations. For example, the read/write heads of many AIT systems do wear and replacement costs of the heads must be addressed in the budget to maintain the AIT system.

C.   SUMMARY

This chapter focused on acquisition policy in DoD and on an acquisition methodology to acquire AIT resources. The key to any acquisition process is understanding the link between the various information systems and the AIT resources that can be used to solve problems, increase productivity, improve quality, provide better management of resources, improve processes, and be a cost effective solution to meet mission requirements. By understanding the present acquisition policies and identifying the resources available to develop an acquisition plan for the organization, the acquisition personnel can identify where and how to get started, how to identify an effective AIT system for their particular application, and obtain practical experience from expert personnel on the AIT system implementation do's and don'ts. An understanding of the application, the process, and the various available equipment resources must be obtained before identifying which AIT resources are most suitable for the particular application. Identification of alternative AIT technologies should be considered in any FEA, cost-performance, and/or cost-benefit analyses. [DEPT94]

The initial system should be structured so new applications can be easily integrated into the system. A modular system design should be sought to add changes when needed without disturbing other applications and/or requiring the cards to be re-issued. The migration plan should have an identified process to develop new functionality considerations as additions to the existing integrated system, rather than modifying the system. [EYES94] Other issues facing DoD include budget and funding considerations, conducting FEAs or other cost-benefit analyses on the different AIT card systems, concern for privacy of data and individual carried data store, and various hardware/software requests. DoD personnel must identify legacy systems, plan for migration to more enhanced automated technologies, and establish target dates for the evaluation and implementation of new systems. Re-engineering and retrofitting processes should be addressed to ensure the acquired card system is used to its fullest potential. [TMIS94, pp. 17-23]

VII. CONCLUSIONS AND TOPICS FOR FUTURE RESEARCH

AIT card technologies are a valuable resource we use in our everyday lives to conduct business transactions and to track various data and assets in various applications. These technologies play a key role in how and when data transactions take place, what data can be stored for various on-line and off-line applications, and why and where the data will be stored for the most beneficial use. Designers, system integrators, information systems management personnel, users and consumers of this technology play a key role in understanding and determining what technologies will be the most effective to use in an application. The designers, system integrators, and systems management personnel play a key role in designing and implementing the AIT card technology systems. The users and consumers play a key role in the use of the card system for the various applications. Therefore, the present and future use of AIT resources will continue to evolve and play an increasing role in our lives as we progress in this "Information Age."

A. CONCLUSIONS

The objective of this thesis research was to identify the various AIT resources available for automation of various applications and to develop matrices to assist personnel making decisions to use these technologies. The matrices are the AIT Functional Capability Matrix and the AIT Card Technology Application Matrix. Both matrices have different purposes to assist a person in the decision making and acquisition process of AIT resources.

The development of the matrices required an extensive literature search, attendance at various AIT resource conferences, and communications with expert personnel, manufacturers and vendors of the AIT resources. This information was presented in Chapter II and Chapter III to inform the reader of the various technologies, their characteristics, their capabilities, and their various applications. From this information, the matrices were developed.

The following sections outline the conclusions drawn from the development and use of the matrices.

1. AIT Functional Capability Matrix Conclusions

The AIT Functional Capability Matrix is designed in a format to provide general functional capability information about the AIT resources and to make a general comparison of the AIT resources with reference to these functional capabilities. This is a present view of the AIT technologies as they exist, their characteristics, their functional strengths and weaknesses, and their application areas. In addition, the matrix was designed in a manner that other functional capabilities and AIT resources can be added as these capabilities and resources evolve. This matrix was designed to consolidate the wealth of information into a usable and coherent format for easy reference of the functional capabilities of these technologies.

By understanding the application requirements to automate an identified system, a system designer can focus on the AIT technology that will best meet these requirements. Information systems personnel must be aware that as the AIT resource functional capabilities evolve over time, some of the characteristics will remain inherent in the media, whereas other characteristics might change and make the AIT a viable option in various uses and application for which it limited capabilities previously restricted its use or application.

The conclusions identified from developing this matrix include:

- security capability of the AIT resource is important in the system design and application environment. This includes the use of cryptographic techniques, PIN, password protection, biometric and voice recognition technologies for user authentication, and hologram,
- logic capability is an important feature to have with interactive AIT card systems,
- multiple technologies can be applied to one card, the "hybrid" card, to maximize the functional capabilities of the card system,
- infrastructure established for use of some AIT card media affects the use and acceptance of other AIT card media (e.g., magnetic stripe vs. integrated chip technologies),
- a phased-in approach to spur societal use and acceptance of the integrated chip technology will require the use of a magnetic stripe with an integrated chip on one card,
- the increase of data storage capacity of the AIT card technologies has and will continue to evolve,

136

- card system costs should address cost per byte of data storage, equipment, system integration, and telecommunication costs and various other functional capabilities of the AIT card media.
- the user base can influence and affect the total card system operation and maintenance costs, (e.g., 100,000 versus 1000)
- centralized and decentralized database system operation affect AIT selection,
- durability and survivability of the AIT technology is extremely important for various environmental considerations,
- interoperability and compatibility issues of the AIT resource should be addressed, and
- future migration of the AIT resources is important in system design considerations.

In review, identifying a viable AIT resource for an application does required a thorough knowledge of the AIT resource and the system application with much foresight to project the future of the AIT resource and the system application. The investment of time and energy to thoroughly research the AIT resource must be undertaken to develop the best system to meet the identified mission need. The final implementation goal should be to use the AIT system to the maximum extent and in various application areas to maximize the return on investment of these technologies.

2. AIT Card Application Matrix Conclusions

The development of the AIT Card Application Matrix in this fashion yielded many avenues to approach identifying how and where AIT resources have been applied. These avenues include use of the matrix to

- identify an application of interest and facilitate choosing an AIT card technology,
- identify the AIT card technologies used for various card system applications, and
- identify applications that can support a "Hybrid" card technology implementation.

The matrix can also be used to address trends and migration information among the various AIT resources. The observed trends include:

- non-logic cards systems to intelligent, logic-capable card technology systems
- no or low security capability to enhanced security capability of the card system

- small data storage capacity to large data storage capacity
- the movement from centralized database use to decentralized database use
- older technologies to the use of newer, more recently developed technologies
- the infrastructure, bar code and magnetic stripe technologies were used in many card applications

The matrix can be used to identifying AIT card technology implemented in specific applications or can be used to focus a system designer or information system management personnel on related application areas where this technology can be used. The matrix was designed in a manner that other applications and AIT resources can be added as these systems and resources evolve. This matrix was designed to consolidate the wealth of information into a usable and coherent format for easy referencing of automated applications using these technologies. From the development of this matrix, the established infrastructure of bar code and magnetic stripe card technologies have and will continue to have a place in AIT card system applications. As the infrastructure is established for the other AIT card technology, new application areas will continue to be identified.

By associating dates or time period to specific applications identified in the AIT Card Application Matrix, a tracking or forecasting approach can be established to identify the potential migration of AIT card technologies. Therefore, understanding the nature of the application environment is a key factor in the selection and acquisition strategy of an AIT card technology used to automate an application.

B.   TOPICS FOR FUTURE RESEARCH

Several topics for future research can be derived from this study of AIT resources, and AIT card systems and their applications. All of the recommended research topics are related to various aspects of AIT systems.

A hybrid card technology with a Code 39 bar code, a magnetic stripe, an integrated chip, and a photograph (being applied to one card) is being researched for use in the government services. Specifically, the DoD project is the Multi-Application Card Reader (MARC) card and the Army project is the Soldier Readiness Card (SRC). Identify and work

with DoD and Army personnel to conduct studies and program assessment of the various applications of this hybrid card technology.

Various applications of the AIT technologies have been used in logistics applications and MITLA projects, to include use of RF/ID and optical laser card technology and/or RF/ID and bar code technology. Identify the various components involved in these applications and conduct assessments on the additional uses of these technologies.

Various AIT functional capabilities continue to change to meet current and projected future needs. A present concern of AIT card systems includes the migration of the card technology emerging faster than it can be evaluated, selected, and acquired. Identify migration strategies, criteria to use in card system migration planning that can assist designers, developers, and implementers of AIT systems.

Various legacy systems exist in DoD. With the reduction in personnel resources, identify legacy systems in DoD that need to be reviewed and reengineered, and assess the potential use of AIT card technologies as the means to automate processes in these operations.

There are various analysis tools available for use in conducting assessments of the automation technologies. Conduct functional economic analysis (FEA), establish criteria to conduct function point analysis, and/or conduct cost-benefit analysis to identify the best methodology to use in assessing AIT resources for certain application environments.

Security and privacy of data are critical issues in any automated process that deals with personnel data and/or classification of information (e.g., INFOSEC). Conduct research on the various security programs (e.g., DES, RSA, etc.) and authentication techniques where AIT resources can be used to address some of these security or privacy of data concerns.

This is a small list of recommendations for continued research with AIT resources. As DoD progresses in re-engineering and automation of processes and applications, the use of these resources will continue to evolve. A prudent research effort to identify other areas to implement this technology can yield many benefits to DoD and other government services.

APPENDIX A: STRENGTHS AND WEAKNESSES OF AIT RESOURCES

Table 10: Bar Code Technology Strengths and Weaknesses

STRENGTHS	WEAKNESSES
• Simple technology • Proven technology • Various symbologies to meet user needs • Various media uses (plastic, cardboard, fabric, metal) • Established standards • Passive operation • Centralized database use • Write once, read many (WORM) technology • Card cost - cheap compared to other card technologies ($0.10 to $0.25 per card) • Interfaces with other equipment (scanner, decoder) •Remaining space on the card available for other uses	• Security - not effective security features on the card • Easily duplicated or counterfeited • Limited data storage capacity • Limited flexibility for various uses • Susceptible to environmental factors affecting the card media

Table 11: Magnetic Stripe Card Technology Strengths and Weaknesses

STRENGTHS	WEAKNESSES
• Proven technology • ISO standards in place • Infrastructure well established • Considered low risk technology • Coercivity features for security capabilities • Multiple tracks for various uses • Many vendors • Card cost - cheap compared to other card technologies (Low density $0.50-$1.00, high density $0.85-$1.50) • Many application areas • Mainly passive media (centralized database use) • Remaining space on the card available for other uses	• Security - magnetically volatile • Easy to alter or duplicate • Limited data storage capabilities (150-475 characters) • Lack of logic capabilities for security control • Active/passive media (lack of distributed database use) • Mechanical failure of read/writer mechanism affects card use • Reader/writer head gap requirements • Susceptible to environmental variations of the card medium (temperatures, chemicals) • Affected by bending, scratches, dirt particles, other magnetic material

Table 12: RF/ID Card Technology Strengths and Weaknesses

STRENGTHS	WEAKNESSES

• Flexibility of placement of read/write media
• No line-of-sight requirements
• Readability characteristics (various frequencies)
• On-the-fly identification
• Password security on the tag (by partition)
• Accuracy of the data (Error detection and correction)
• Data storage capacity (from 8 bytes to 128 KB)
• Multiple design features to meet user requirements
• Unlimited application areas
• Interactive or passive media
• Centralized or decentralized uses
• Contactless capabilities
• Tolerance for use in various environmental conditions
• Draft standards (RF/ID)
• Interfaces to various other media/equipment
• Increases productivity
• Increases customer service response time
• Reduces paperwork, space and time requirements
• Host computer systems can provide logic capability for tag use
	• Read/write interference of metallic objects
	• Lack of logic capabilities on the tag itself
	• Cost compared to other technologies (high)
	   (varies with storage capacity - $5 to $125 per card)
	• Requires more sophisticated hardware and software
	• Maintenance of operation when host system fails
	   (address this for all technologies in chap 6.)

Table 13: Optical (Laser) Card Technology Strengths and Weaknesses

STRENGTHS	WEAKNESSES
•Data storage capability (6.6 MB +) •Error Detection and Correction (EDAC) features •Write once, read many technology (WORM) •Security capabilities •Audit trail capabilities •Durable •EMI resistant •ISO/ECI standards and ANSI draft standards •Environment variation tolerance •Active and passive media (for centralized and decentralized use) •Various applications •Interfaces to various other equipment (scanner, camera) •Reverse of card available for other uses	•Cost compared to other technologies ($5.00 to $8.00 per card) •Requires more sophisticated hardware and software •Infrastructure for technology not in place • Equipment not very portable, sensitive to movement

Table 14: Smart Card Technology Strengths and Weaknesses

STRENGTHS	WEAKNESSES

•High security capabilities (encryption capabilities)
•Logic/Intelligence
•High data storage capability (2KB to 64KB+)
•Read/write capabilities
•Flexibility (multiple application uses)
•Audit trail capabilities
•Interactive operation (active and passive media)
•Programmability
•Tamperproof, practically impossible to forge or alter
•ISO and draft ANSI standards
•Durable (contactless card medium)
•Accurate, timely data transaction
•Interfaces to various other equipment (scanner, camera)
•Many application areas
	•Cost compared to other technologies
	  ($5.00 to $25.00 per card)
	•Requires more sophisticated hardware and software
	  devices and interfacing software
	•Infrastructure for technology not in place
	•Privacy of personal information is major worry
	•Environmental susceptibility (contact card medium)

Table 15: PCMCIA Card Technology Strengths and Weaknesses

STRENGTHS	WEAKNESSES
•Multiple applications (various types for various uses) •High data storage capacity (1MB to 80+ MB) •Read/write operational capability •Active and passive media •Software program capabilities •Security features (software program development) •Ease of use •Flexibility (various types) •Excellent growth potential •Backward compatibility •Interfaces with other equipment (notebooks, PDA, etc.) •Draft standards •Open systems capability features	•Cost compared to other technologies (base on application: $80 to over $1000 per card) •Requires more sophisticated hardware and software •Interoperability issues •Incompatibility concerns •Lack standards •Infrastructure not established for total acceptance of use •Not a proven technology (for all features discussed) •Power (voltage) requirements •Electromagnetic interference (affects card information) •Environmental tolerances (temperature, chemicals, etc.)

Table 16: MICR and OCR Technology Strengths and Weaknesses

STRENGTHS	WEAKNESSES
• Write once, read many (WORM) technology • Simple technology • Proven technology • Infrastructure established • Many vendors produce product/product services • Established standards • Mainly passive media (centralized database use to recognize characters) • Cost of the technology can be cheap (depends on application) • Interfaces with other equipment (scanner, decoder) • Remaining space on the media available for other uses	• Lack security capability • Easy to alter, duplicate or counterfeit (fraudulent use) • Limited data storage capacity • Lack of logic capability • Limited flexibility for various uses • Susceptible to environmental factors affecting the media to which it is written (temperature, chemicals)

Table 17: Biometric and Voice Data Technology Strengths and Weaknesses

STRENGTHS	WEAKNESSES
•High security capabilities •Various biometric ID and voice data technologies •Various vendor sources •Can be used in active and passive operating systems •Used on various media (bar code, smart card, etc.) •Interfaces to various other equipment (scanner, camera) •Voice recognition system can require minimal training •Real time data collection •Various measures of effectiveness	• No standards • Cost of the various systems (depends on system) • Requires more sophisticated hardware and software

Table 18: Machine Vision Technology Strengths and Weaknesses

STRENGTHS	WEAKNESSES
• Operate without human intervention • Monitor and control robotic activity • Read-oriented technology • Can facilitate decision making • Can be used where other AIT can not be used • Interfaces with other equipment (scanner, camera, etc.) • Associated media strengths (bar code, OCR)	• Cost • Requires more sophisticated hardware and software • No standards for system development/implementation • Associated media (bar code, OCR) weaknesses

APPENDIX B: FUNCTIONAL CAPABILITY CRITERIA DEFINITIONS

Applicability: Able to be applied; appropriate, suitable, fitting, to put to or adapt for a special or specific use. [WEBS88, p. 119]

Audit trail: A means for identifying the actions taken in processing input data or in preparing output. By use of the audit trail, data on a source document can be traced to a specific output, and an output can be traced to the source items from which it was derived. The chronological set of records that provide evidence of system activity. [WNWD88, p. 18] The records can also be used to track system usage and detect and identify intruders. [RUSS91, p. 399]

Compatibility: The ability of different devices, such as a computer, a printer, or a card system, to work together. [WNWD88, p. 58] The capability of two or more items or components of equipment or material to exist or function in the same system or environment without mutual interference. [Joint Pub 6-0, p. II-3]

Cost: An amount paid or to be paid for the purchase of a product. [WEBS88, p. 316] The cost is evaluated in monetary terms and will be based on the dollar value per byte of data storage capacity of the card/tag media.

Counterfeit: To make a copy of, usually with the intent to defraud, forge; cause deception, fraudulently or deceptively imitate. To make an imitation of what is genuine with the intent to defraud, a fraudulent imitation or facsimile. [WEBS88, p. 319]

Data Storage Capacity: Capability of a data storage device to store large quantities of characters/bytes, of data. [WNWD88, p. 93] The amount of data that can be stored on the medium, measured in kilobytes (K) or megabytes (MB). A kilobyte is 1024 bytes of data and a megabyte is 1,048,576 bytes of data. One byte is 8 data bits. For data storage, higher capacity is important for storing high volumes of data. [GAO90, p. 15]

Duplication: To copy so that the result remains in the same physical form as the source; for example, to make a new diskette with the same information and in the same format as an original diskette. [WNWD88, p. 122]

Durability: Capable of withstanding wear and decay. [WEBS88, p. 411] Durability includes capability to withstand bending, scratching, dirty/dusty environments, magnetic fields, severe impact, chemical solvents, and various environmental tolerances, e.g., physical conditions of temperature, humidity, and so forth. The environment may affect operational efficiency. [WNWD88, p. 133] Environmental conditions include various temperature (degree of hotness or coldness, e.g., extremes temperatures of -40° to 200°), harsh terrain, and various weather conditions. [INFO94, p. 15]

Ease of Use: A term applied to hardware or software that allows a user to operate the equipment or software with little or no instruction, e.g., user-friendly. [WNWD88, p. 397]

Electromagnetic Interference (EMI): Electromagnetism is the magnetism arising from an electric charge in motion, the physics of electricity and magnetism, containing a specific amount of electromagnetic energy. Electromagnetic spectrum is the total range of radiation which includes cosmic-ray photons, gamma rays, x-rays, ultraviolet radiation, visible light, infrared radiation, microwaves, radio waves, heat, and electric currents. [WEBS88, p. 422] The author considered permanence - a measure of the ability of a magnetic circuit to conduct magnetic flux - within this functional characteristic. [WEBS88, p. 875]

Error detection: A process in which each expression conforms to specific rules of construction. When expressions occur that do not conform to the rules of these constructions, an error is indicated. A single error-detecting code produces a forbidden combination if a digit gains or loses a single bit. [WNWD88, p. 135] It can also be used in terms of the bit error-rate, e.g., the probability of a bit of data delivered from the device being incorrect. [GAO90, p. 15]

Flexibility: Responsive to change, adaptable. [WEBS88, p. 487] Flexibility is required of systems to meet changing situations and diversified operations with a minimum of disruption and delay. It can be obtained by system design (standardization), using commercial facilities, mobile or transportable systems, or pre-position facilities. [Joint Pub 6-0, p. II-3]

Growth Potential: The process of growing, full development: maturity; development from a lower or simpler to a higher or more complex form: evolution; an increase, as in size, number, value, or strength: expansion; the result of growth: production. [WEBS88, p. 551]

Human Intervention: Also known as "human-machine interface," the boundary at which people interact with machines. [WNWD88, p. 177] The use of a human being to interact between two or more objects or media for interaction of the objects/media to occur.

Information Security (INFOSEC): Protection of information. The government program whose focus is the techniques that increase the security of computer systems, communications systems, and the information they process or transmit. [RUSS91, p. 408]

Infrastructure (established): An underlying base or foundation; the basic facilities, equipment, and installations needed for the functioning of a system. [WEBS88, p. 628]

Interactive (Active) Operation: An action results in response to outside simulation. [SVIG87, p. 194] Yielding an immediate response to input. The user or operator is in direct, two-way, continual communication with the computer system and/or its components. An

operator can modify or terminate a program and receive feedback from the system for guidance and verification. [WNWD88, p. 192]

Interoperability: The condition achieved among various systems, items, or equipment when information or services can be exchanged directly and satisfactorily between them and their users. All aspects of achieving interoperability must be addressed throughout the life cycle of the system. Aspects include doctrine, concepts, operational procedures; identification, coordination, review, and validation of requirements; development and validation of interoperability standards; acquisition; testing, verification, enforcement of interoperability standards; system and standards configuration management; and joint/combined training and evaluation. [Joint Pub 6-0, p. II-2]

Line of Sight: An unobstructed path between electronic sending and receiving antennas. [WEBS88, p. 696]

Logic Capability: Intelligence of the system or item to provide and/or follow a sequence of instructions for performing a specific job or task, make logical choices, follow alternative decision paths, and to recognize and respond to externally provided information. [SVIG87, pp. 1, 201] The basic principles and application of truth tables and the interconnection among logical elements required for arithmetic computation in an automatic data processing system. [WNWD88, p. 214]

Mechanical device contact for read/write operation: The mechanical nature of the read/write head requiring contact with the card media for read/write operation. Direct read/write head contact with the card media can affect the operation life cycle of the card media. Mechanical data processing is a method of data processing that involves the use of relatively small and simple (usually non-programmable) mechanical machines. [WNWD88, p. 230]

Multiple medium use: Medium is defined as the physical substance upon which data is recorded, such as floppy disks, magnetic tapes, and paper. [WNWD88, p. 230] Other media includes plastic, cardboard, and labels.

Open System Capability: Compatible with various systems, systems designed around standards that let them be expanded in many directions e.g., non-proprietary. [PALM91, p.193] Enables dissimilar computers to exchange information and run on each other's software. Open systems provide the flexibility to upgrade with relatively inexpensive, off-the-shelf components. [CORB93, p. 28]

Operational Characteristic: A specific characteristic that, when used, can initiate, modify, or stop a control operation. [SIPP81, p. 361] The author defines operational characteristic as a distinguishing attribute or element which controls or directs the functioning of an object or a process, in this case the operational characteristics of card media.

Passive Operation: Receiving or subjected to an action without responding or initiating a corresponding action, accepting without resistance or objection; non participating, acting, or operating: inert; submitted without objection or resistance. [WEBS88, p. 859] A passive device is a device that passes signals without altering them. [WNWD88, p. 276]

Proven Technology (mature): A technology that is readily available on the commercial market and that has been in operational use in many installations over a substantial period of time. For card technologies, a mature medium is important to ensure that it can be kept and used easily and accurately over a long period of time. [GAO90, p. 15]

Risk: Possibility of suffering harm or loss: danger; a factor, course, or element involving uncertain danger; expose to a chance of loss or damage; endanger. [WEBS88, p. 1013]

Security features (physical): Freedom from danger, harm, or risk of loss: safety; the degree to which a program or device is free from unauthorized use; prevention of unauthorized use of a program or device; measures adopted to guard against attack or disclosure. [WEBS88, p. 1055] Security involves the measures taken to achieve a reasonable freedom from criminal, fraudulent, and vandalizing actions while maintaining sensitivity to unexpected attacks or system failures that cannot be distinguished from attacks. [SVIG87, p. 204]

Simple Technology: Having or composed of one or a few things or parts; not complex: easy; without additions or modifications; without embellishment; not elaborate, elegant, or luxurious. [WEBS88, p. 1085]

Standards: A rule established to describe how the technology is designed, developed, and implemented on the various media [GAO90, p. 15] to improve the quality of information system development and operation, uniform practices and common techniques. A guide or yardstick used to measure performance of any computer system function. A standard may be laid down by a statutory body or simply created by a major manufacturer's practice [WNWD88, p. 358], e.g., International Standard Organization (ISO) and American National Standard Institute (ANSI) defined standards. Standards are important to support various system uses to ensure compatibility. [GAO90, p. 15]

Survivability: Built-in features, functions, and characteristics that help to assure that a card will last through its intended life [SVIG87, p. 204]; remain in existence; to persist through. [WEBS88, p. 1166]

Tamper: To interfere in a harmful way, to meddle foolishly or rashly, to alter improperly; to handle something idly, ignorantly, or destructively. [WEBS88, p. 1182]

Vendor: A manufacturer of data-processing products. [SVIG87, p. 205] A vendor can be a company or business entity that sells computers, peripheral devices, time-share services, or computer services or a supplier. [WNWD88, p. 400]

148

APPENDIX C: AIT FUNCTIONAL CAPABILITY MATRIX INFORMATION

1A-1F: Applicability (for various applications): The baseline established to summarize applicability is: rating of 1 = low applicability for various applications to a rating of 3 = high applicability for various applications.

1A-1F: A rating of 3 is assigned for all of the AIT card technologies. All of the AIT resources having applicability for various applications as noted in Chapter 3.

2A-2F: Data Storage Capability: The baseline established to summarize data storage capability was defined from no (0 byte) data storage capability to the megabyte (MB) and higher ranges for data storage capability of the AIT card technologies. A rating of 1 = low data storage capability (from 0 to 1K), a rating of 2 = average data storage capability (1K to 1MB), and a rating of 3 = high data storage capacity (above 1MB). See Figure C-1.

DATA STORAGE CAPABILITY
(byte or character)

0   1K   1 MB

Section 1 = Rate 1 (low) | Section 2 = Rate 2 (avg) | Section 3 = Rate 3 (high)

I- Mag. Stripe ►
I- Bar Code
I- Smart Card
I- RF/ID
I- Optical (laser) Card
I- PCMCIA Card

AIT CARD TECHNOLOGIES
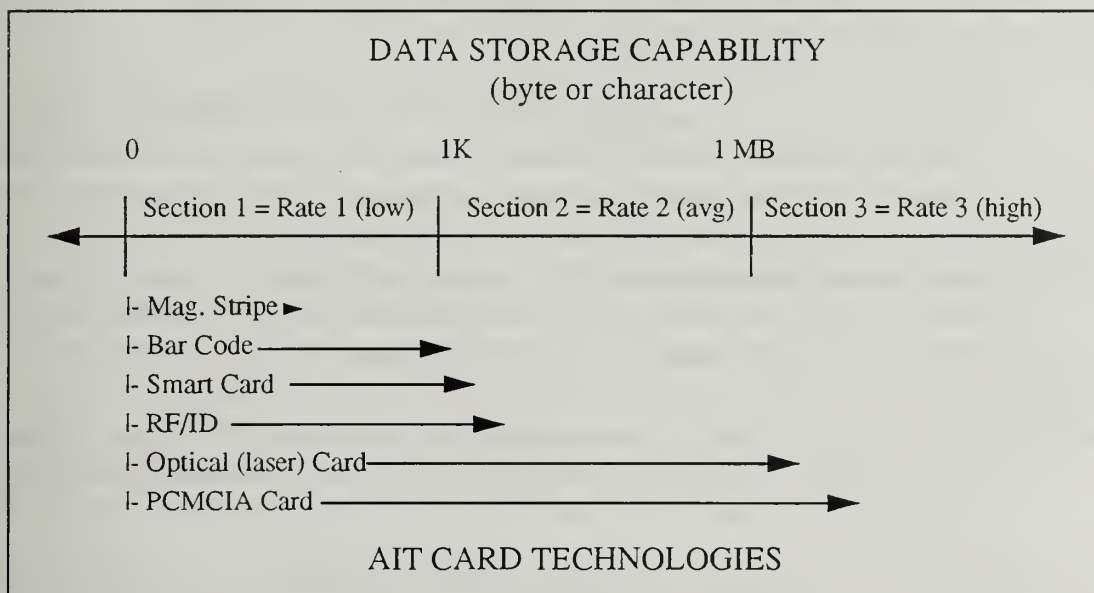
Figure C-1: Data Storage Capability (by byte or character)

2A: A rating of 2 is assigned to bar code technology. Bar codes have various storage capabilities based on the symbology used: MIL-STD-1189B recommends a maximum of 32 characters for Code 39 bar code symbology, including start, stop, and other control bits. [MIL-STD-1189B, p. 13] [MARC, p. 4] Reference sources stated typically 24 characters are considered the norm when using this bar code symbology. [REBO94] [ZAGU94] PDF 417 bar code can store over 2K bytes. [ITKI92]

149

2B: A rating of 1 is assigned to magnetic stripe technology. The data storage capacity is 150 characters for low density magnetic stripe and 475-500 characters for high density magnetic stripe. [INFO94, pp. 22, 24] Other references identified the data storage capacity for magnetic stripe at < 100 bits. [HADD93, pp. 381, 389]

2C: A rating of 2 is assigned to smart card technology. Smart card data storage capacity can be 2KB to 64KB. [INFO94, p. 24]

2D: A rating of 2 is assigned to RF/ID technology. RF/ID data storage capacity can range from less than 200 bits [HADD93, p. 389] and 8 KB [INFO94, p. 24] up to 128KB. [VOSS94, p. 390]

2E: A rating of 3 is assigned to optical card technology. Optical card data storage capability can be 2.8 MB with EDAC to 4.1 MB without EDAC [INFO94, p. 15] up to 6.6 MB. [SPAR94, p. 323]

2F: A rating of 3 is assigned to PCMCIA card technology. PCMCIA data storage capability can be up to 64 MB. [HADD93, p. 389]

3A-3F: **Ease of Use**: The baseline established to summarize ease of use (by the users) is: rating of 1 = difficult to use (low desired capability) to a rating of 3 = easy to use (highly desired capability).

3A-3F: A rating of 3 is assigned to all of the AIT card technologies. All the AIT card technologies seemed to be easy to use. This rating was assigned based on the author's observation of operation and contact with AIT card system experts.

4A-4F: **Electromagnetic Interference**: The baseline established to summarize card media affected by electromagnetic interference (EMI) is: rating of 1 = low resistance of card media to EMI to a rating of 3 = high resistance of card media to EMI.

4A, 4D, 4E: A rating of 3 is assigned to bar code, RF/ID and optical card technologies. The bar code and optical card are not affected by EMI. [INFO94, p. 15] and RF/ID signals can not be erased by strong magnetic fields [TUTT94, p. 361].

4B, 4C, 4F: A rating of 1 is assigned to magnetic stripe, smart card and PCMCIA technology. The magnetic stripe [PALM91, p. 9], smart card [SVIG87, p. 43], and PCMCIA card technologies are affected by EMI.

4C: A rating of 1,2 is assigned to smart card technology. The rating of 1 is assigned to the contact smart card since it is susceptible to EMI due to the exposure of the contacts [SVIG87, p. 43]. The rating of 2 is assigned to the contactless smart card since it has some immunity to EMI. [MITG93]

5A-5F: **Error Detection (transmission/reception) Capability**: The baseline established to summarize error detection capability is: a rating of 1 = no or low error detection capability to a rating of 3 = high error detection capability.

5A, 5C-5E: A rating of 3 is assigned to bar code, smart card, RF/ID and optical card technologies. Bar code systems can have error detection information as part of the protocol used in transmission/reception process.Error correction and detection algorithms, data protection and encryption functions can be designed into the smart card systems. [SVIG87, pp. 59-60] [BRIG92, p. 30] [PALM91, p. 175] RF/ID is extremely accurate with calculated error rates as low as 1 in 100 trillion. [TUTT94, p. 361] Optical cards have EDAC capability. [INFO94, p. 15] [DREX92]

Note: Quantitative information for error detection was available for some AIT resources, but not all of them. The author inferred a level of error detection capability based on the available information found in the research effort. Research on some AIT resources did not provide enough information for the author to assign a value for this functionality criteria, therefore no value was assigned.

6A-6F: **Flexibility (for various applications)**: The baseline established to summarize flexibility is: rating of 1 = not or low flexibility for various applications to a rating of 3 = very flexible for various applications.

6A: A rating of 2 is assigned to bar code technology. The bar code was considered to have average flexibility. It has limited data storage capacity and it can not be rewritten. A new bar code tag must be printed and/or attached to the object. [MILS93, p. 230] [LAIR94]

6B-6F: A rating of 3 is assigned to magnetic stripe, smart card, RF/ID, optical card and PCMCIA card technologies. These technologies have rewrite, reusability, and/or large data storage capability to support their flexibility for use in various applications. [SVIG87, pp. 36, 47-48] [RIST93, p. 275]

7A-7F: **Growth Potential/Expandability**: The baseline established to summarize growth and expandability potential is: a rating of 1 = no or very little or low growth and expandability potential to a rating of 3 = unlimited growth and expandability potential.

7A-7F: A rating of 3 is assigned to all of the AIT resources. All of the AIT resources were considered to have excellent growth and expandability potential for future applications, potentially larger data storage capabilities, interface capabilities with other technologies, and proven standards with an established infrastructure in future years.

8A-8F: Line-of-Sight Operational Requirement (between card and read/write system): The baseline established to summarize line-of-sight operation requirement is: N = not required and R = required.

> 8A-8F, except 8C (contactless) and 8D: A rating of R is assigned to bar code, magnetic stripe, smart card (contact), optical card, and PCMCIA card technologies. These card technologies require direct line-of-sight, with some card systems requiring actual read/write head contact, between the card and the read/write system for operation.
>
> 8C (contactless), 8D: Ratings of N and R are assigned to contactless smart card and RF/ID technologies. Based on the application of the smart card and RF/ID technologies, they can operate with or without direct line-of-sight between the tag and the reader/writer system for operation. [TUTT94, p. 361] Contactless smart cards have been used in toll road applications. [ATT93]
>
> Note: With specific applications of card technologies (e.g., optical card) integrated with RF systems, the line-of-sight characteristic can change.

9A-9F: Logic/Decision Making Capability: The baseline established to summarize logic capabilities is: rating of 1 = no or low logic/decision making capabilities to a rating of 3 = high logic/decision making capabilities.

> 9A-9F, except 9C: A rating of 1 is assigned to bar code, magnetic stripe, RF/ID, optical card, and PCMCIA card technologies. These technologies do not have an integrated chip and do not have logic capabilities build onto the card.
>
> 9C: A rating of 3 is assigned to the smart card technology. The smart card has an integrated chip that can be designed for logic capability (provide and follow instructions, make logical choices, to follow alternative decision paths, and to recognize and respond to externally provided information). [SVIG87, p. 1]

10A-10F: Mechanical Device Contact for Read/Write Operation (direct): The baseline established to summarize mechanical device contact for read/write operation is used to address contact requirement and how the read/write device can affect card operation, e.g., the direct contact can create wear with the media and can affect its operation life cycle. A rating of 1 is assigned to the card technologies requiring mechanical read/write device contact. A rating of 3 is assigned to the card technologies that do not require direct mechanical read/write device contact. Because read/write device interaction can create wear and reduce the operation life of the card medium, it is considered a low functional capability when compared to the card technologies that do not require contact and will not create wear or reduce the operation life of the card media, a high functional capability to have in the card system.

10A, 10C (contactless), 10D, 10E: A rating of 3 is assigned to bar code, contactless smart card, RF/ID, and optical card technologies. Bar code uses a laser beam or scanning device for read operation. The scanning device does not need physical contact with the bar code to operate. [DAVI91, p. 12] A contactless smart card does not have its leads exposed to the read/write heads for card operation. [HADD93, p. 385] RF/ID uses radio frequency transmissions for read/write operations. [DAVI91, p. 30] The optical card uses a laser beam for read/write operations. [CANON] [DREX92]

10B, 10C (contact), 10F: A rating of 1 is assigned to magnetic stripe, contact smart card, and PCMCIA card technologies. The magnetic stripe has read/write head contact for operation. [PALM91, p. 9] A contact smart card has its leads exposed and the read/write device must interact with the card for card system operation. [HADD93, p. 385] PCMCIA card has read/write head contact for card operation. [ZIFF94, p. 1] [HADD93, p. 389]

Note: The notation of 1,3 in cell 10-D of the matrix is used to distinguish contact and contactless smart card technologies functional characteristics. The first number identifies the rating for contact smart card technology, the second number identifies the rating for contactless smart card technology. Therefore, the functional capability is identified in one cell for the technology.

11A-11F: **No Human Intervention Required**: The baseline established to summarize no human intervention required is: rating of 1 = card technologies that required human intervention for the card to operate to a rating of 3 = card technologies that required no human intervention for the card to operate. The functional capability of the systems that require human intervention are identified as low compared to the functional capabilities of the system that require no human intervention. Various reasons for this rating scale are identified below. See FIgure C-2.
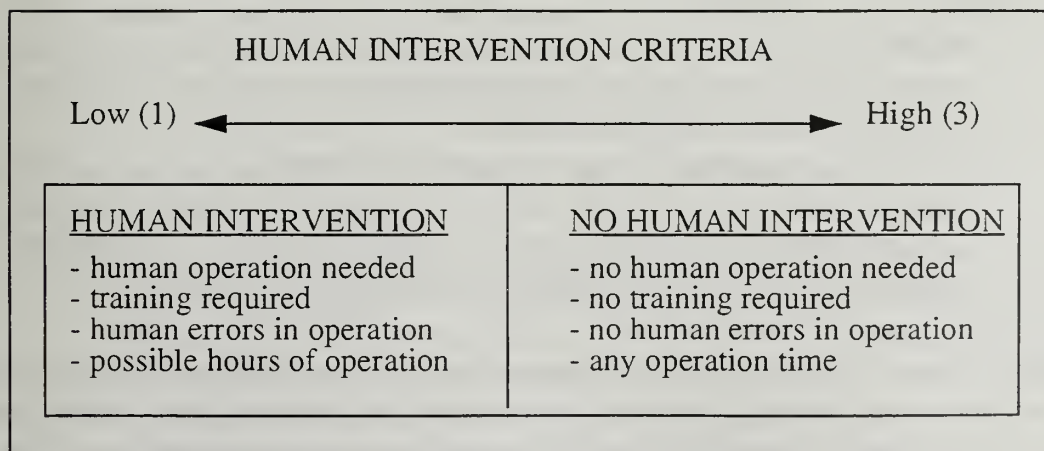
Figure C-2: Human Intervention Criteria Consideration

11A, 11B, 11C (contact), 11E, 11F: A rating of 1 is assigned to bar code (not associated with machine vision systems), magnetic stripe, smart card (contact), optical card technology (not integrated with RF systems), and PCMCIA card technologies. These technologies required human intervention of placing the card in the read/writer system or operating some mechanism for some system action to occur. [PALM91, p. 9]

11A, 11C (contactless), 11D, and 11E: A rating of 3 is assigned to bar code, smart card (contactless), RF/ID, and optical card with RF/ID system. These technologies can operate without human intervention, a computer system can be programmed to activate their operations. [MILL94, p. 232] [ATT93] For example, the bar code can be applied in machine vision systems which do not required human intervention [INTERMEC] and optical cards can be integrated with RF/ID systems to enhance its application in this area. [CAPA94, p. 294]

12A-12F: **Open System Capability**: The baseline established to summarize open system capability is: rating of 1 = proprietary, not open system capability to a rating of 3 = open system capability.

12A-12F: A rating of 3 is assigned to all the AIT card technologies. With draft and established standards and a multitude of vendors producing the various card technologies, the card technologies are acquiring open system compatibility with other systems. [PALM91, p. 193]

13A-13F: **Interactive Operation (for decentralized database use)**: The baseline established to summarize interactive operation (decentralized database use, read/ write operations) is: rating of 1 = can not be used or is a weak media to use in interactive operations to a rating of 3 = can be used for interactive operation.

13A-13B: A rating of 1 is assigned to bar code and magnetic stripe card technologies. These AIT card technologies have limited data storage capability which limits their use for decentralized database applications. [INFO94, p. 23] [SVIG87, p. 27] [PARK94, p. 646]

13C-13F: A rating of 3 is assigned to smart card, RF/ID, optical card, and PCMCIA card technologies. These AIT card technologies have read/write and large data storage capabilities for decentralized database applications. [PARK94, p. 646] [MILS93, pp. 235-236] [CAPA94, p. 294] [RIST93, p. 264]

14A-14F: **Passive Operation (for centralized database use)**: The baseline established to summarize passive operation use (centralized database use, mainly reading operations) is: rating of 1 = can not be used for passive operations to a rating of 3 = passive operation use.

154

14A-14F: A rating of 3 is assigned to all the AIT resources. Bar code and magnetic stripe card technologies are mainly used for passive operations. [INFO94, p. 23] [SVIG87, p. 27] [PARK94, p. 646] The other AIT card technologies can be used for passive or interactive operations. [SVIG87, p. 52][MILS93, pp. 235-236]

15A-15F: **Proven Technology**: The baseline established to summarize proven technology is: rating of 1 = not proven technology with few years of use to a rating of 3 = proven technology with years of use. See Figure C-3.

EVOLUTION OF AIT RESOURCES

Capability = 3

(Proven technology. In use/existence for over 20 years. Infrastructure well established. Many installed applications.)

Capability = 2

(Somewhat proven technology. In use/ existence for < 20 years.)

Capability = 1

(New technology. Not proven, typically still in testing phase.)

1940   1950   1960   1970   1980   1990   2000

Year

I- RF/ID
I- Bar Code
I- Magnetic Stripe
I- Smart Card
I- Optical
I-PCMCIA

AIT CARD TECHNOLOGY

Figure C-3: Evolution of AIT Resources

15A-15B, 15D: A rating of 3 is assigned to bar code, magnetic strip, and radio frequency technologies. These technologies have been proven, have been in existence for many years, and are considered to be mature technologies, compared to optical card, smart card, and PCMCIA cards. Bar coding has been in existence since 1949 in the grocery business [PALM91, pp. 11-14], magnetic stripe have been in the used as a Financial Transaction Card (FTC) since 1969 [SVIG87, p. 165], and RF/ID has been in existence since WWII. [TUTT94, p. 361]

15C, 15E -15F: A rating of 2 is assigned to smart card, optical card, and PCMCIA card technologies. Smart card was developed in the early 1970s [WON91, p. 4], optical card was developed in 1981 [KEAB92, p. 38], and PCMCIA was developed in 1989 [RIST93, p. 264]. Smart cards have been in existence for 20 years, but they have had less use/existence compared to bar code, magnetic stripe, and RF/ID technologies. The use of these technologies has been growing in recent years.

16A-16F: **Security Features (physical, built-in) Available**: The baseline established to summarize available physical security features is: rating of 1 = no or low available physical security features, rating of 2 = some physical security features available, to a rating of 3 = available physical security features.

16A-16B: A rating of 1 is assigned to bar code and magnetic stripe card technologies. These technologies have no or low physical, built-in security features. [HADD93, pp. 381, 386, 389] [INFO94, p. 24]

16C-16F: A rating of 3 is assigned to smart card, RF/ID, optical card and PCMCIA card technologies. Smart cards can have the physical, built-in security features. [HADD93, pp. 383, 389] [INFO94, p. 24] [PARK94, p. 646] RF/ID tags can be enclosed in non-metallic casing and still function. [DAVI91, p. 30] Optical cards can tolerate various environmental conditions and is EMI-resistant. [CANON] [DREX92] [CAPA94, p. 294] PCMCIA cards are constructed with a plastic frame, and covered on both sides by stainless steel panels, making the cards robust, rigid and durable vessels for sensitive components and the PCMCIA cards have options for security features. [HADD93, p. 389]

17A-17F: **Audit Trail Capability**: The baseline established to summarize audit trail capability is: rating of 1 = no audit trail capabilities (low desired capability) to a rating of 3 = audit trail capability (highly desired capability).

17A-17B: A rating of 1 is assigned to bar code and magnetic stripe technologies. These technologies have very little data storage space and do not have audit trail capabilities on the card themselves. (Note: The audit trail capabilities can be developed in the software and used from a centralized database environment, but the audit trail is not capable of being on the card itself.) [INFO94, p. 23]

17C, 17E: A rating of 3 is assigned to smart card and optical card technologies. These technologies have large data storage and audit trail capabilities that can store the audit trail on the card. [SVIG87, p. 59] [INFO94, p. 15]

18A-18F: **Information Security (resistance to duplication, counterfeit, tamper)**: The baseline established to summarize information security (duplication/counterfeiting) is: rating of 1 = duplication/counterfeiting possible to a rating of 3 = resistance to duplication/counterfeiting.

18A-18B: A rating of 1 is assigned to bar code and magnetic stripe card technologies. These technologies are susceptible to duplication, counterfeiting, and tampering leading to fraudulent use. [INFO94, pp. 22, 23] [PARK94, p. 646]
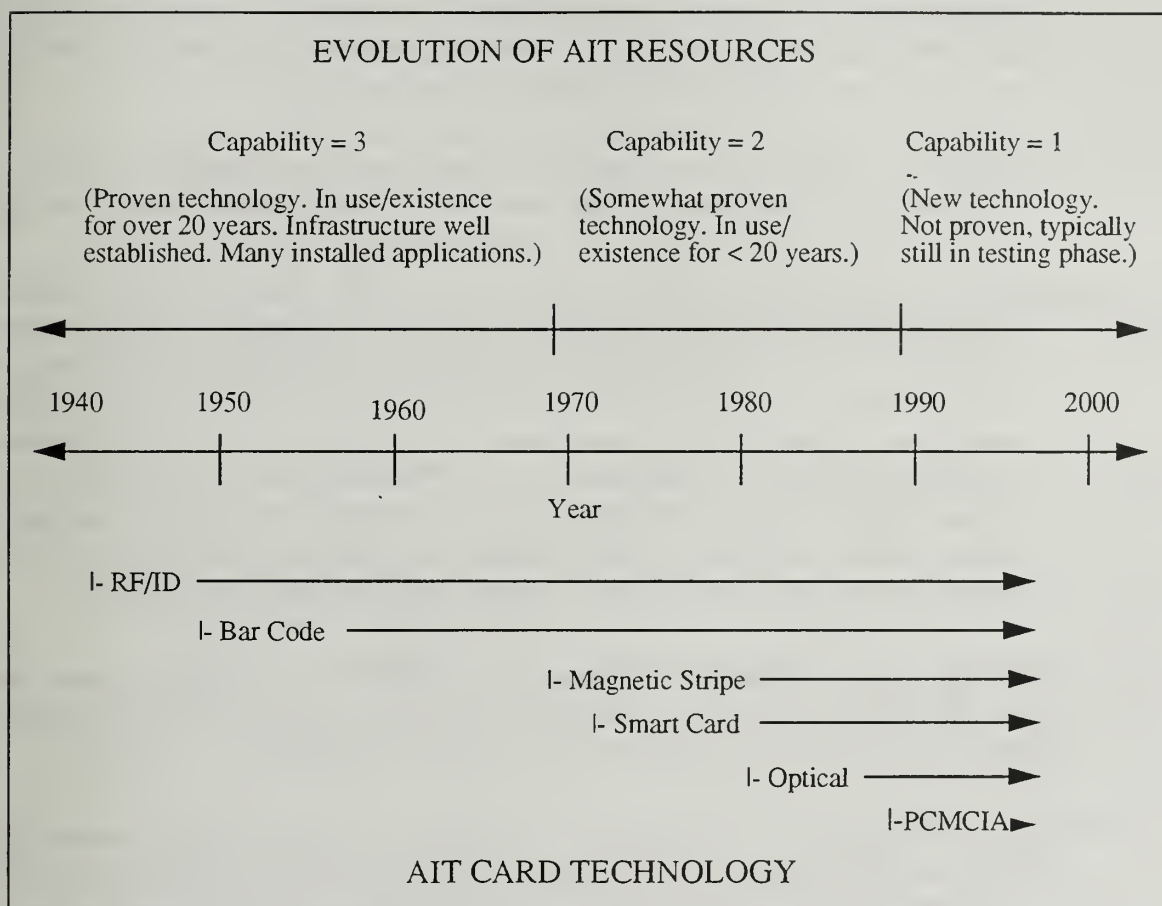
18C-18F: A rating of 3 is assigned to smart card, RF/ID, optical card, and PCMCIA card technologies. These technologies are less susceptible to duplication, counterfeiting, and tampering. Smart cards and PCMCIA cards can have security algorithms or other security measures implemented on the card to provide information security. [PARK94, p. 646] [HADD93, pp. 384, 389] RF/ID tags can be password protected and are less susceptible to counterfeiting. [TUTT94, pp. 361, 365] Optical cards retain any changes to the card, so the card can be checked for unauthorized changes through the audit trail capabilities [INFO94, p. 15] and data encryption programs can be associated with optical card systems.

19A-19F: **Survivability**: The baseline established to summarize survivability is: rating of 1 = low survivability resulting from lack of durability characteristics to a rating of 3 = survivability with durability characteristics.

19A-19B, 19C (contact smart card): A rating of 1 is assigned for bar code, magnetic stripe, and contact smart card technologies. [LAIR94] [TUTT94, p. 361] [SVIG87, pp. 42-46, 119] [PARK94, p. 646] Use of adhesives, label substrates, and environmental conditions affect the use of bar code technology in various applications. In addition, the bar code must be verified to ensure its legibility for continued use. [LAIR94] The contact smart card can be affected by various conditions due to the exposed lead/pin connections. [HADD93, pp. 385, 389]

19C (contactless smart card), 19F: A rating of 2 is assigned for contactless smart card and PCMCIA technologies. A contactless smart card is resistant to dirty environments, but operation of the card can be affected by bending and scratches if the integrated chip (s) on the card is damaged. [HADD94, p. 385] [SVIG87, p. 119] [PARK94, p. 646] PCMCIA cards are constructed with a plastic frame, and covered on both sides by stainless steel panels, making cards into robust, rigid and durable vessels for sensitive components. PCMCIA card with its exposed lead/pin connections can be affected by various environmental and chemical factors. [HADD93, pp. 385, 387, 389]

19D, 19E: A rating of 3 is assigned for RF/ID and optical card technologies. These technologies are very durable and can survive a variety of conditions. [INFO94, p. 15] [TUTT94, p. 361]

20A-20F: **Cost (Dollar/Byte or Character)**: The baseline established to summarize cost was based on the dollar cost per byte or character of data that can be stored on the

card. A rating of 1 = high dollar cost per byte of data storage capability to a rating of 3 = low dollar cost per byte of data storage capability. See Figure C-4.

DOLLAR COST PER BYTE OR CHARACTER

<-------------Rating = 3------------->|<-------Rating = 2 ------->|<-----Rating = 1--->

$0.000001 $0.00001 $0.0001 $0.001 $0.01 $0.10

I-Optical card-I   I-------------- Bar Code -------------I

I-PCMCIA card-I   I---Smart Card---I

I-Magnetic-I
Stripe
I----------- RF/ID --------I

AIT CARD RESOURCES
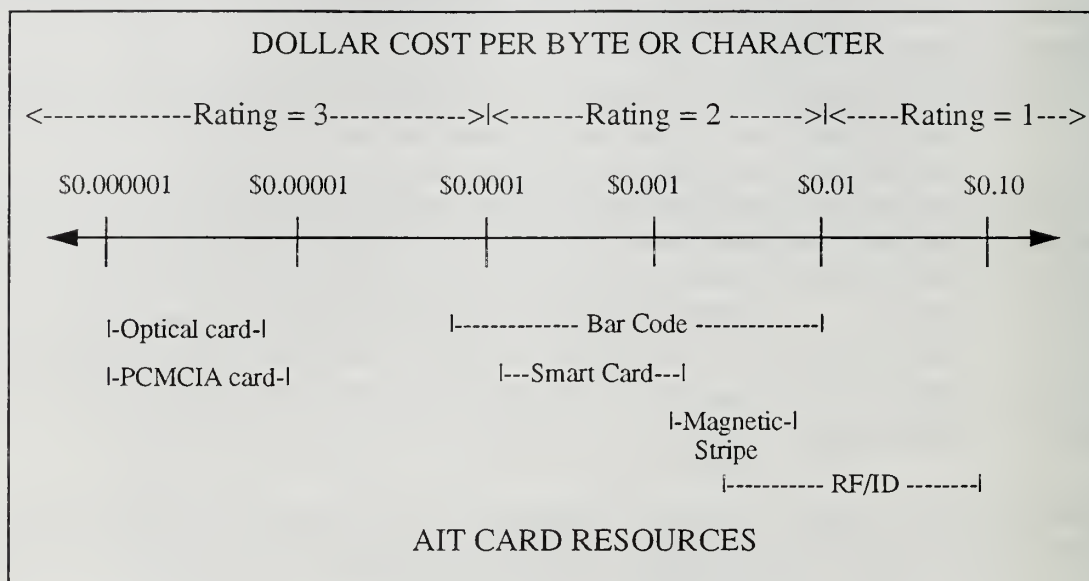
Figure C-4: Dollar Cost per Byte or Character

20A: A rating of 1,2 is assigned to bar code technology for card application. Cost of bar code on a card was identified as $0.10 to $0.25 per card [INFO94, p. 24] and the data storage capacity used was 24 byte for Code 39 (MIL STD 1189) [PALM91, p. 31] to over 2K for PDF 417. [ITKI92]

20B: A rating of 2 is assigned to magnetic stripe technology for card application. Cost of the magnetic stripe card was identified as $0.50 to $1.50 per card and data storage ranged from 150 to 475 characters. [INFO94, p. 24] [HADD93, pp. 381, 389]

20C: A rating of 2 is assigned to smart card technology for card application. Cost of the smart card was identified as $5.00 to $25.00 per card and data storage capacity was 8KB to 64KB [INFO94, p. 24] Some individual costs were $1.45 -$1.80 for 1K EPROM serial memory up to $9.00-$26.10 for 8KB EEPROM with microprocess. [SEID94, p. 208]

20D: A rating of 1,2 is assigned to RF/ID technology for card/tag application. Cost of the RF/ID card/tag was identified as $5 to $20 per card [HADD93, p. 389] for less than 200 bytes data storage capacity, $100 to $125 per card/tag for 8KB data storage capacity [INFO94, p. 24], and $190 per card/tag for 128KB data storage capacity. [DOD94]

20E: A rating of 3 is assigned to optical card technology for card application. Cost of the optical card was identified as $5.00 to $8.00 per card and data storage capacity was 2.8MB to 4.2MB. [INFO94, p. 24]

20F: A rating of 3 is assigned to PCMCIA technology for card application. Cost of the PCMCIA card was identified as $80.00 per card and higher (depending on the application and data storage was 64MB. [HADD93, p. 389]

Note: The information provided in [INFO94, p. 24] was based on a general range of dollar costs to the general range of available data storage capacity of the card technologies. The actual dollar cost and specific data storage capability of the card technologies would be within this range. Consideration must be given to the specific technology/symbology used. For example, a 1-D bar code (e.g., Code 39) would be cheaper to produce than a 2-D bar code (e.g., PDF 417). [ALSB94]

21A-21F: **Infrastructure for Technology Well Established**: The baseline established to summarize the technology infrastructure is: rating of 1 = infrastructure not well established to a rating of 3 = infrastructure well established.

21A-21B: A rating of 3 is assigned to bar code and magnetic stripe technologies having an well established infrastructure. [TUTT94, p. 361]

21C, 21E-21F: A rating of 1 is assigned to smart card, optical card and PCMCIA card technologies. These technologies have been in existence for 20 years or less and the infrastructure is not well established in the United States and the world for world-wide use in comparison to bar code and magnetic stripe. [PARK94, p. 647] [RIST93, p. 265]

21D: A rating of 2 is assigned to RF/ID technology. This rating was based on the existence of RF/ID since WWII. [TUTT94, p. 361] It has been used in various application so some infrastructure was assumed to exist for this technology.

22A-22F: **Simple Technology/Low Risk**: The baseline established to summarize the technologies as simple, low risk to complex, high risk is: rating of 1 = complex, high risk to a rating of 3 = simple, low risk.

22A-22B: A rating of 3 is assigned to bar code and magnetic stripe card technologies for simple/low risk technologies. [INFO94, pp. 22, 23] [PALM91, p. 8]

22C-22F: A rating of 2 is assigned to smart card, RF/ID, optical card, and PCMCIA card technologies. These card technology systems are more complex to develop and implement and they have various additional interfaces and operational considerations for their use. [TUTT94, pp: 361] [HADD93, p. 389]

23A-23F: **Standards Established (ISO, ANSI, etc.)**: The baseline established to summarize whether established standard existed for the various technologies is: rating of 1 = no established standards to a rating of 3 = established standards.

23A-23F: A rating of 3 is assigned to all of the AIT card technologies. All of the AIT card technologies have established or draft standards in place for their use. [PALM91, pp. 21-59] [INFO94, pp. 15-24] [SVIG87, pp. 23, 154-159] [CARN94, p. 360] [CALL94, pp. 317-320] [GEMPLUS, pp. 1-33] [RIST93, pp. 263-272]

24A-24F: **Compatibility/Interoperability with other equipment**: The baseline established to summarize compatibility/interoperability is: rating of 1 = not compatible/interoperable with other equipment to a rating of 3 = compatible/ interoperable with other equipment.

24A-24B, 24D: A rating of 3 is assigned to bar code, magnetic stripe, RF/ID technologies. Tight specifications of optical properties and range of dimensions, equipment (e.g., scanner) can be of a compatible form. [PALM91, p. 193] In addition, there is an established infrastructure, many vendors, and various applications of these technologies. RF systems have compatibility with other technologies, such as bar code, optical card, and contactless smart card applications. [PALM91, p. 181] [CAPA94, p. 294] [ATT] Draft interface standards can affect compatibility with other systems. [HADD93, p. 386]

24C, 24E: A rating of 2 is assigned to smart card and optical card technologies. Smart card manufacturers and vendors are not alike, which affects the compatibility and interoperability of the various card and card systems. [SEID94, p. 211] These technologies are beginning to mature and compatibility and interoperability issues are being address. Smart card technology has recently been interfaced on a card with bar code and magnetic stripe technologies. [MARC] Optical card technology has been interfaced with RF technology. [CAPA94, p. 294] With these technologies being interfaced with other systems, compatibility will be a key feature in the card use.

24F: A rating of 2 is assigned to PCMCIA card technology. There are still some compatibility issues that must be addressed, which include chip incompatibilities, Card and Socket Services software, and enabler drivers that affect the use of PCMCIA cards in various systems. [RIST93, pp. 265, 267, 270]

25A-25F: **Use of Various Media (plastic, cardboard, etc.)**: The baseline established to summarize use of various media is: rating of 1 = use of one media to a rating of 3 = use of various media for the card material. See Figure C-5.

```
+-------------------------------------------------------------+
|                  VARIOUS MEDIA CRITERIA                     |
|  Low (1)  <------------------------------->  High (3)       |
|   +-----------------------+---------------------------+     |
|   | FEW MEDIA             | MANY MEDIA                |     |
|   |                       | - paper                   |     |
|   | - plastic             | - plastic                 |     |
|   | - optical media       | - cardboard               |     |
|   |                       | - labels                  |     |
|   |                       | - tags                    |     |
|   +-----------------------+---------------------------+     |
+-------------------------------------------------------------+
```
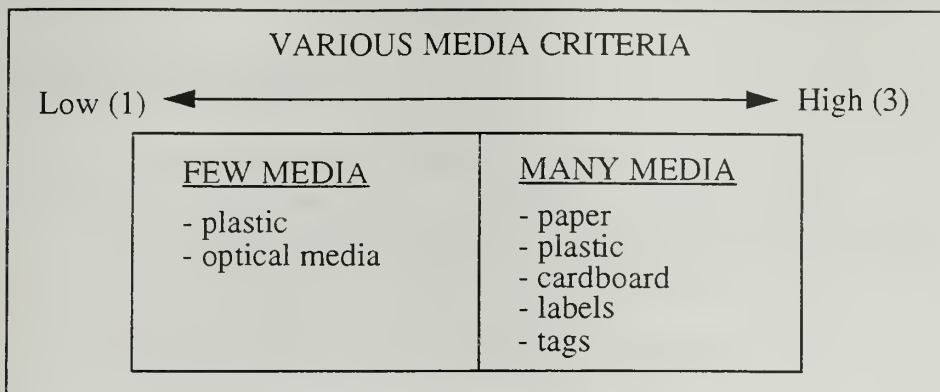
Figure C-5: Media Criteria

25A-25B, 25D: A rating of 3 is assigned to bar code, magnetic stripe, and RF/ID technologies. [INFO94, pp. 19, 23] [get other references (ms)]

25C, 25E-25F: A rating of 1 was assigned to smart card, optical card, and PCMCIA card technologies. These card technologies have one or two media of which the card is made/packaged, mainly plastic media (smart card, PCMCIA) and optical media (optical card). [SVIG87, pp. 42-46] [HADD93, p. 387]

26A-26F: **Vendors (few to many):** The baseline established to summarize vendor support issues is: rating of 1 = proprietary, few vendors to a rating of 3 = many vendors.

26A-26B, 26C, 26F: A rating of 3 is assigned to bar code, magnetic stripe card, smart card, and PCMCIA technologies. Many vendors support these technologies. [INFO94, pp. 17, 22, 23] Smart cards adhere to international standards, ensuring multiple-vendor sources and competitive prices. [PARK94, p. 646]

26D, 26E: A rating of 2 is assigned to RF/ID and optical card technologies. These technologies have various vendors supporting the technology, but not as many as bar code or magnetic stripe technologies. The author made this observation from attending various conferences and through the literature search.

APPENDIX D: AIT CARD APPLICATION MATRIX INFORMATION

1A-1H: Access Control/Security

    1A: Bar code technology: [FMS90, p. 213]
    1B: Magnetic stripe technology: [FMS90, p. 165] [RUSR91]
    1C: Smart card technology: [FMS90, p. 138] [BROW88] [SANT92]
    1D: RF/ID technology: [CUSH94, p. 346] [FMS90, p. 54]
    1E: Optical card technology: [SOLT94]
    1G: Biometric technology: [DAVI91, p. 14] [FMS90, p. 7]

2A-2H: Campus Card (Student, Faculty, Support Personnel)

    2A: Bar code technology: [FMS90, pp. 196, 237]
    2B: Magnetic stripe technology: [FMS90, pp. 196, 237]
    2C: Smart card technology: [FMS90, p. 237]
    2G: Biometric technology: [FMS90, p. 237]

3A-3H: Document Storage Card

    3E: Optical card technology: [LATA85] INFO94, p. 13]
    3F: PCMCIA technology: [RIST93, p. 266]

4A-4H: Electronic Certification System

    4C: Smart card technology: [FMS90, p. 40]

5A-5H: Electronic Ticketing Collection (ETC) (sporting events, plays, theaters, etc.)

    5B: Magnetic stripe technology: [FMS90, p. 237]
    5C: Smart card technology: [FLOO92]
    5G: Biometric technology: [FMS90, p. 237] [FLOO92]

6A-6H: Employee Card (Time, Attendance)

    6A: Bar code technology: [FMS90, pp. 25, 64]
    6B: Magnetic stripe technology: [FMS90, pp. 22, 23, 58, 64]
    6C: Smart card technology: [WON91, p. 5]
    6D: RF/ID technology: [CUSH94, p. 346]

7A-7H: Financial: Accounting System

      7A: Bar code technology: [FMS90, pp. 132-133]
      7B: Magnetic stripe technology: [FMS90, p. 42]
      7C: Smart card technology: [FMS90, p. 90]

8A-8H: Financial: Automatic Teller Machine (ATM)

      8B: Magnetic stripe technology: [SVIG87, p. 21]
      8C: Smart card technology: [HOFN92]

9A-9H: Financial: Credit Collection/Authorization Card

      9B: Magnetic stripe technology: [FMS90, p. 10]

10A-10H: Financial: Electronic Benefits Transfer (EBT)

      10A: Bar code technology: [FMS90, p. 100]
      10B: Magnetic stripe technology: [FMS90, pp. 98, 99, 107, 110, 127, 141, 151, 255-257]
      10C: Smart card technology: [FMS90, pp. 190, 212, 258-259] [WON91, p. 11] [IACO91] [MCCR92]

11A-11H: Financial: Prepaid Cash/Debit/Stored Value Card

      11A: Bar code technology: [FMS90, pp. 117-118]
      11B: Magnetic stripe technology: [FMS90, pp. 16-17, 44, 77,] [HOLL93, pp. 26-29] [MURP92]
      11C: Smart card technology: [MART89]

12A-12H: Health Services: Health Service Card (Patient care, Medicaid)

      12A: Bar code technology: [PALM91, pp. 205-206]
      12B: Magnetic stripe technology: [FMS90, pp. 144-145, 163]
      12C: Smart card technology: [DANI91] [DCPR84] [SANT92] [HOFN92]
      12D: RF/ID technology (monitoring): [CUSH94, p. 346]
      12E: Optical card technology: [INFO94, p. 13] [KAYE94, p. 305]
      12G: Biometric technology: [HOFN92]

13A-13H: Health Services: Insurance Card

      13B: Magnetic stripe technology: [JOHN91]
      13C: Smart card technology (unemployment insurance): [MCCR92]

14A-14H: Health Services: Pharmacy Card

    14B: Magnetic stripe technology: [FMS90, pp. 206-207]
    14C: Smart card technology: [WON91, p. 13]

15A-15H: Library Card System

    15A: Bar code technology:[INFO94, p. 23] [PALM91, p. 195] [FMS90, p. 196]
    15C: Smart card technology: [SMIT87]
    15D: RF/ID technology: [CUSH94, p. 346]
    15E: Optical card technology: [SPEC93, pp. 218-219]

16A-16H: Logistics (Inventory/Material/Fuel Control, Mobility)

    16A: Bar code technology: [FMS90, pp. 60, 66, 67] [PALM91, p. 196]
        [INTERMEC]
    16B: Magnetic stripe technology: [FMS90, pp. 21, 197, 210, 255-257]
    16C: Smart card technology: [FMS90, pp. 28, 35, 36, 37, 54, 63, 160, 258-259]
        [WON91, p. 7]
    16D: RF/ID technology: [FMS90, pp. 28, 30, 32, 54, 63, 257-258] [CUSH94,
        p. 346]
    16E: Optical card technology: [CAPA94, p. 294]

17A-17H: Manufacturing Operations (includes maintenance, quality assurance)

    17A: Bar code technology: [PALM91, p. 198]
    17C: Smart card technology: [FMS90, pp. 36-37] [SANT92]
    17D: RF/ID technology (QA data): [FMS90, p. 65]
    17E: Optical card technology (maintenance): [KAEB92]
    17H: Machine vision technology: [INTERMEC]

18A-18H: Marketing Operations (Trade Show, Convention)

    18C: Smart card technology: [LAUG93]

19A-19F: Personal Identification and Management:

    19A: Bar code technology: [DODP94, p. F-7] [FMS90, p. 79]
    19B: Magnetic stripe technology: [FMS90, pp. 7, 79, 255-257]
    19C: Smart card technology: (MARC and SRC)[FMS90, p. 54] [MARC94]
    19D: RF/ID technology: [CUSH94, p. 346]
    19E: Optical card technology: [SOLT94] [INFO94, p. 13]
    19G: Biometric technology: [DAVI91, p. 14] [INFO94, p. 20]

20A-20H: **Resource Management [Forestry, Licensing (Fish, Hunt), Dog Management Programs]**

    20C: Smart card technology: [FMS90, pp. 56-57, 96-97, 226-227]
    20D: RF/ID technology: [FMS90, pp. 55-56]

21A-21H: Retail Applications (retail, supermarket purchases, valued customer)

    21A: Bar code technology: [PALM91, p. 203] [FMS90, pp. 59-60]
    21B: Magnetic stripe technology: [MURP92] [KASS92]
    21C: Smart card technology: [GATE90] [SANT92]
    21D: RF/ID technology: [CUSH94, p. 346]
    21E: Optical card technology: [KAEB92]

22A-22H: Services: Agriculture/USDA/Farm Quota System

    22C: Smart card technology: [WON91, p. 9] [FMS90, pp. 2-3] [SANT92]
    22D: RF/ID technology: [CUSH94, p. 347]

23A-23H: Services: Educational Service/Training/ Job Placement

    23C: Smart card technology: [WON91, pp. 9-11]

24A-24H: Services: Pay Telephone

    24B: Magnetic stripe technology: [BASS93]
    24C: Smart card technology: [BAND91] [BASS93]
    24E: Optical card technology: [BASS93]

25A-25H: Services: Parcel Tracking and Post Office System

    25A: Bar code technology: [INTERMEC]
    25B: Magnetic stripe technology: [FMS90, p. 24]
    25D: RF/ID technology: [CUSH94, p. 346]
    25H: Machine vision technology: [INTERMEC]

26A-26H: Services: School Lunch Debit Card Program

    26B: Magnetic stripe technology: [FMS90, pp. 112-113, 139, 224]

27A-27H: **Transportation: Drivers Licensing/Vehicle Registration/Vehicle Identification**

27B: Magnetic stripe technology: [FMS90, pp. 102, 218]
27D: RF/ID technology: [CUSH94, p. 346]
27G: Biometric (fingerprint, signature): [FMS90, p. 102]

28A-28H: **Transportation: Electronic Toll Collection (ETC) and Traffic Control (road, bridge, airport; vehicles (cars, trucks, bus), train, and parking meter systems)**

28A: Bar code technology: [FMS90, pp. 133-134] [HOFI92]
28B: Magnetic stripe technology: [MURP92]
28C: Smart card technology: [FLOO92] [TORE93] [WON91, pp. 12-13]
28D: RF/ID technology: [FMS90, pp. 136-137, 182, 217, others (257-258)] [CUSH94, pp. 346-347]

29A-29H: **Transportation: Weigh Station Processing**

29D: RF/ID technology: [FMS90, p. 167] [CUSH94, p. 346]

30A-30H: **Other product application: Modem/Fax Applications**

30F: PCMCIA technology: [RIST93, p. 266]

31A-31H: **Other applications as products: Network Interface Application**

31C: Smart card technology (Network access): [ROTH93]
31F: PCMCIA technology (LAN Adapter card): [TABI93, p. 275]

32A-32H: **Other applications as products: Secure Telephone Unit (STU)**

32C: Smart card technology: [FMS90, pp. 72, 75]

APPENDIX E: GLOSSARY OF TERMS

Access Control   Controlled access to premises, equipment (computer), and services.

Active   Powered card, on board battery to support RAM, processor, display, input keyboard, and operating system.

ANSI   American National Standards Institute. A private organization that coordinates some United States standards-making. Represents the United States to the International Standards Organization.

Authentication   The process of proving that a subject (e.g., a user or a system) is what the subject claims to be. Authentication is a measure used to verify the subject's eligibility and the subject's ability to access certain information. It protects against the fraudulent use of a system or fraudulent transmission of information. There are three classic ways to authenticate oneself: something you know, something you have, and something you are.

Badge   An information carrying identification device that usually contains a photo and is traditionally displayed.

Bar Code   A series of vertical bars that contrast with the background. Usually black on white. These bars and spaces of specific widths are arranged in a unique sequential pattern to represent binary data.

Barium Ferrite   Permanent magnetic material "Read Only" placed on a card to form a binary code. Usually used as Access Control cards.

Biometric   The use of unique, quantifiable physiological, behavioral, and morphological characteristics to prove positive identification. Examples include fingerprints, thumbprints, hand geometry, voiceprints, eye retina patterns, and DNA.

Bandwidth   The amount of data that can be moved through a particular communications link.

Bit   One binary digit that can be either "0" or "1."

BPI   Bits per inch, a measure to identify the storage of binary information, as on a magnetic stripe card.

BPS   Bits per second. Transmission speed over some media.

Byte   A unit that represents 8 bits.

Card (ISO)	Can be any information carrying device that conforms to the ISO height and width standard dimensions.
Cash Card	A pre-paid credit balance stored on a card. Such card systems decrement the balance with each use.
Card Security	A unique property integrated into the card or stripe material that can be detected, digitally read, and used to "secure soft data" on the card. A card can be associated with algorithmically linked systems with encoded data, thus making corruption of the data difficult.
Card Transport	A motorized device that moves the card through a read and/or write cycle and returns the card to the user.
Certification	The technical evaluation performed as part of, and in support of, the accreditation process that establishes the extent to which a particular computer system or network design and implementation meets a set of security requirements.
Challenge-Response	A type of authentication in which a user responds correctly (usually be performing some calculation) to a challenge (usually a numeric, unpredictable one).
Channel	A path used for information transfer within a system.
Check Sum	Numbers summed according to a particular set of rules and used to verify that transmitted data has not been modified in transmission.
Coercive Force	The energy required to saturate a given piece of magnetic material. Measured in oersteds.
Coercivity	The magnetic "retention value" of different ferrous oxide materials.
Computer Security	Protection of information while it is being processed or stored.
Configuration Mgmt.	The identification, control, accounting for, and auditing of all changes to system hardware, software, firmware, documentation, test plans, and test results throughout the development and operation of a system.
Core Material	The centerpiece of the card that gives the card its characteristic features.
Cryptography	The study of encryption and decryption.
Degauss	Demagnetize magnetic media in a way that leaves very low residue of magnetic induction on the media. Effectively erases the data.

Density	The number of data bits per inch (BPI) with reference to magnetic stripe recording material.
DES	Data Encryption Standard A private key encryption algorithm adopted as the federal standard for the protection of sensitive unclassified information and used extensively for the protection of commercial data as well. A public domain algorithm.
Digital Signature	An authentication tool that verifies the origin of a message and the identity of the sender and receiver. Can be used to resolve any authentication issues between the sender and the receiver. The digital signature is unique for every transaction.
Digitizing	Converting a graphic image into a "digitized" form. The digitized form becomes a graphics file that can be electronically stored and retrieved.
EEPROM	Electronically Erasable Programmable Read Only Memory, also known as "E squared PROM." EEPROM makes it possible to read/write a memory chip.
Electronic Imaging	The act of video "frame grabbing," digitizing, and subsequently placing such image in a file or on a card.
Embossing	A method of "striking" raised characters on plastic or metal. A male or female die set that "squeezes" the material into a character shape.
Encoder	The device that "writes" information to a stripe, card, chip, etc.
Encoding	The act of "writing" information.
Encryption	The transformation of original text (called plaintext) into unintelligible text (called ciphertext). Also called "enciphering."
End-to-End Encryption	A type of encryption where a message is encrypted upon transmission and is decrypted and then encrypted again each time it passes through a network communication node. Also called "online encryption."
EPROM	Electrically Programmable Read Only Memory (UV light to erase).
Erasure	Removal of signals recorded on magnetic media.
Ergonomics	The study of equipment design in order to reduce operator fatigue and discomfort.

Ferrous Oxide	The metal "rust" particles that are used to make magnetic stripes. The controlled rusting (oxidation) determines the recording characteristics of the magnetic material.
Financial Card	Cards that are used to determine eligibility for debit/credit financial services.
Font	Character configuration, usually refers to OCR technology.
Hologram	Unique photographic printing that gives an image a three dimensional effect. Usually employed for security or aesthetic effect.
Holographic	A method of encoding that embodies a three dimensional binary bit that is recognized by a special reader.
I.C.	Integrated circuit or "chip."
Identification	The process of telling a system the identity of a subject (e.g., a user or another system). Usually, this is done by entering a name, password, PIN, or presenting a token to a system.
Identification Card	"I.D." Cards. Cards that usually carry identifying characteristics (e.g., photo, height, color of eyes) of the cardholder. Cards that identify the bearer as eligible for specific services.
IEEE	Institute of Electronic and Electrical Engineers. A leading standard-making body in the United States, responsible for the various electrical engineering standards.
Image File	Usually a compressed digitized photo. Could also be photo, signature, and fingerprint maintained in a single file. Such files are used for card issue/re-issue and security access.
Information Security	Protection of information. (INFOSEC)
Intelligent Card	Memory card with a processor.
ISO	International Organization for Standards, also known as International Standards Organization.
KB	Kilobyte means 1024 bytes (2^{10} bytes). With smart card, a "K" usually means kilobits.
Key	In cryptography, a secret value used to encrypt and decrypt messages. The sequence is known only to sender and receiver of the message.

Laminate	The process of combining the overlay and substrate materials by using heat, time and pressure.
Laser Card	"Laser" equates to high density optical recording. The term "Laser Card" is a proprietary name used by the Drexler Corporation.
Machine Readable	A code or characters that can be read by machines.
Magnetic Stripe	Magnetic material conforming to the ISO standards for size, position, and magnetic characteristics.
MB	Megabyte means 1,048,576 bytes (2^{20} bytes)
Mbps	Million bits per second. 2^{20} bits of information (usually used to express a data transfer rate; as in, 1 megabit/second - 1 Mbps).
Memory	Any storage of data, such as Read-Only Memory (ROM) or Random Access Memory (RAM).
Memory Card	Non-intelligence (no processor) card with data storage capability, such as an EPROM card, magnetic, and optical card.
MHz	Megahertz means million cycle per second
NIST	National Institute of Standards and Technology
Nonce	A word invented or used for a particular occasion.
OCR	Optical Character Recognition
Oersted	A unit of magnetic coercive force. Also used to define relative magnetic material "energy retention value."
Off-Line	In card driven systems, "off-line" is defined as a "Go - No Go" situation resulting from the card having legitimate recognition by the reader or a terminal. An off-line reader or terminal can contain a downloaded file to check eligibility of the cardholder.
Open System Card	Refers to a prepaid card that can be accepted in several environments, e.g., transit, telephone, vending, POS.
On-Line	In card driven systems, "on-line" is defined as in communication with the intelligent host. The host may be a "smart terminal." It may be an "access control controller" that can typically reside on the other side of the wall from the reader. In each case, there is an "interactive" transaction between the host, the card, and the cardholder.

Optical Card	High Density (2-200MB). Usually photo-lithographic process for ROM card. Laser encoding for field read/write.
Overlay	The clear plastic material placed over the printing on the card substrate. Sometimes referred to as "over-laminate."
Passive	Card that needs no power of its own to operate and usually needs no power to read or is powered by the reader.
Password	A secret sequence of characters that is used to authenticate a user's identity, usually during a login process.
PCMCIA	Personal Computer Memory Card International Association.
Photo I.D.	The term "photo I.D." is used to reference a photo on a card, badge, or an electronically stored image that may be retrieved with or without a card.
Physical Security	Protection of physical computer systems and related buildings and equipment from fire, other natural disasters, and intrusion. It covers the use of locks, keys, and administrative measures used to control access to computer systems and facilities.
PIC	Personal Identification Characteristics, such as eye color, height, weight.
Picture Card	A traditional card with a picture of the cardholder on or in the card. Also called a Photo I.D. card.
PIN	Personal Identification Number. A number or code that is unique to the individual and can be used to prove identity. Often used with automatic teller machines (ATMs) and access devices.
Pixel	"Picture element." Referred to video imaging for photo I.D. cards.
Plaintext	In cryptography, the original text that is being encrypted.
POS	Point of sales. The point the card is used for a transaction.
Polyester	A very durable plastic material used in cards and badges. Not usually embossed.
Prepaid Card	A card that stores prepaid value, e.g., telephone cards.
PROM	Programmable Read-Only Memory.

Proximity	A "non contact" system for reading cards. Data is exchanged between the card and the reader by radio frequency, fiber optics, magnetic induction, laser, or other non-mechanical contact technology.
PVC	Poly Vinyl Chloride. A material used in the manufacture of credit and I.D. cards. PVC has certain attributes that allow it to retain a "set" such as embossing. It is printable and will laminate at moderate temperatures.
RAM	Random Access Memory
Read/Write	The act of data that is encoded/re-encoded. Read/write as opposed to read-only as in ROM. The information flows from an object to a subject. In read operations, no alteration of information occurs. In write operations, alteration of information occurs.
Read After Write	A data integrity check. Data is immediately read after it is written and compared to the file that drives the encoder.
ReaderWriter	A device that can encode (write) and read the encoding on a card or badge.
Reader	A device that can read the encoding on a card or badge.
RF	Radio Frequency. Medium that is used for a card to communicate with a reader in a "proximity" or "non-contact" system.
Risk Management	Is the discipline of quantifying the cost of security compromise. Risk management compares the cost of "securing a system" to the perceived cost of loss incurred if the security was not in place. Taking known risks because such risks can be managed in a cost effective way.
ROM	Read-Only Memory
Saturation	In magnetics, a stripe is said to be properly encoded when it is "saturated." The maximum signal strength is achieved when no additional write current improves output.
Secondary Security	A special property, resident in a magnetic stripe card, that is digitized and used to "lock" the encoded data to the card on which it was originally encoded.
Security	Freedom from risk or danger. Safety and the assurance of safety.

Smart Card	Refers to an I.C. card with a microprocessor. The card is used to gain access to a facility or a computer system.
Soft Data	Data that can be easily changed, such as magnetic encoding or EEPROM data storage.
Spot	A term used to describe a high density optical bit. Spots can be as small as one micron.
Stand Alone	(SAL) A device or card that requires no system with which to interface in order to perform a transaction.
Stored Value Card	Same as a "cash card."
Substrate	A core material used for manufacturing a card.
Swipe	The "swipe" refers to the hand motion of moving the card through the reader of a manually operated device.
Token	A physical item that is used to provide identity. Typically an electronic device that can be inserted in a door or a computer system to gain access.
Validation	The performance of tests and evaluations to determine whether a system complies with specifications and requirements.
Visual Data	Eyeball readable information on a card. It can be printed, photographed, copied, and embossed.
Vulnerability	A weakness in a computer system, or a point where the system is susceptible to attack. The weakness could be exploited to violate system security.
Wand	A hand-held device, usually for reading bar codes. The wand must be in contact or near contact with the bar code medium.
Weigand Effect	A combination of magnetic wires imbedded in a card to make a binary machine readable code.
Witnessing	Used to describe the act of a read head, wand, laser beam, or other device actually "locating" data tracks or fields.
WORM	Write-Once Read Many. An example is optical card technology.

These definitions comes from a variety of sources to include [LIND93], [RUSS91], [SVIG87], [WEBS88] and [WNWD88].

LIST OF REFERENCES

[AITC94]   AIT Contract, Contract Number DAHC94-94-D0003, U. S. Army
                Information System Selection and Acquisition Agency, 25 March
                1994.

[ALSB94]   Telephone conversation between W. Alsbrook, Vice President -
                General Manager, National Headquarters, Information Spectrum, Inc.,
                Falls Church, VA and the author, 8 July 1994.

[AMSC93]   "Adapters Make Smart Card Smarter," *AT&T Technology*, v.8, n. 2, p.
                12, Summer 1993. DIALOG file 15, item 00758248.

[ATT93]   AT&T, "Electronic Toll Collection," AT&T Smart Card (Brochure)

[BAND91]   Bandell, P., "Playing Cards," *Telcom World*, p. 35, December 1991.
                DIALOG file 15, item 00597292.

[BASS93]   Bass, P., "Selecting A Card Technology," *CardTech/SecurTech 1993
                Conference Proceedings*, CTST, Inc., p. 375, 18 April 1993.

[BELS93]   Belsie, L., "'Smart Cards' Connect Consumers," *Christian Science
                Digest*, v. 85, n. 181, p. 8, 13 August 1993.

[BRIG92]   Bright, J., "Smart Solutions," *Telecommunications*, International
                edition, v. 26, n. 2, pp. 30, 75-76, February 1992. DIALOG file 15,
                item 00601778.

[BROW88]   Brown, J., "Bank's Smart Cards Offer Tight Security," *Network World*,
                v. 5, n. 21, p. 15, 23 May 1988. DIALOG file 15, item 00407162.

[CALL94]   Callen, R. and Haddock, R., "Optical Card Standards: An Overview,"
                CardTech/SecurTech 1994 Conference Proceedings, CTST, Inc., pp.
                317-320, 10 April 1994.

[CANON]   Canon, *Canon Optical Card System*, Canon, U.S.A., Inc. (Brochure)

[CAPA94]   Capaldi, L. C., "The Defense Logistics Agency (DLA) Automated
                Manifest System (AMS): A Status Report," *CardTech/SecurTech 1994
                Conference Proceedings*, CTST, Inc., pp. 293-304, 10 April 1994.

[CARN94]   Carnes, J. N., "Interface Standards: ANSI ASC X3T6," *CardTech/
                SecurTech 1994 Conference Proceedings*, CTST, Inc., p. 360, 10 April
                1994.

[CART94]   Carter, R., "The Present and Future State of Biometric Technology," *CardTechSecurTech 1994 Conference Proceedings*, CTST, Inc., pp. 401-415, 10 April 1994.

[CASE93]   Casey, J., "EBT System Security - Are We Prepared," *CardTech/ SecurTech 1993 Conference Proceedings*, CTST, Inc., pp. 802-810, 18 April 1993.

[CHAN94]   Telephone conversation between N. Chan, Director of Marketing, SunDisk Corporation, San Jose, California and the author, 15 June 1994.

[CORB93]   Corban, L., "The Byte-Buying Blues," *Government Executive*, pp. 26-28, 31-33, January 1993.

[CUSH94]   Cashing, C., "The Present and Future State of Radio Frequency Identification," *CardTech/SecurTech 1994 Conference Proceedings*, CTST, Inc., pp. 337-353, 10 April 1994.

[DANI91]   Danielle, E., "Smart Cards: Is Off-Line on Target?" *Insurance & Technology*, v. 16, n. 3, pp. 39-45, April 1991. DIALOG file 15, item 00556734.

[DAVI91]   Davis, M. and Morgan, T., "1991/92 Reference Guide & Directory," *Automatic I.D. News*, pp. 12-34, August 1991.

[DATACARD]   DataCard, "DataCard Serial Memory Smart Cards" and "DataCard MIC-1600 Microprocessor Card," DataCard. (Brochures)

[DCPR84]   "Dr. Com Puter's Report: Medical Application of Smart Card," *Medical Computer Journal*, v. 4, n. 1, pp. 8-9, Annual 1984. DIALOG file 275, item 00612714.

[DEPT94]   Department of the Air Force, "Conclusions of Total Asset Visibility (TAV) Conference Technology Panel, Department of the Air Force, Headquarters United States Air Force, Washington, D.C., 14 March 1994.

[DOD94]   Department of Defense Reader Frequency Transponder Contract, Number F33600-94-D0077, April 1994.

[DODI 5000.2] Department of Defense Instruction 5000.2, *Defense Acquisition Management Policies and Procedures*, Under Secterary of Defense for Acquisition (USD(A)), Washington, DC, 23 February 1991.

[DODP94]   "Department of Defense Plan for Action for Two-Dimensional Bar Code Standards," Defense Information System Agency, Joint Interoperability and Engineering Organization Center for Standards Information Processing Directorate, March 1994.

[DREI92]   Dreifus, H. N., "Public Telephone Applications for Card Technologies; Practical Applications, Issues and Future Trends," *Card Tech Conference Proceedings*, pp. 146-156, 7 April 1992.

[DREX92]   Drexler Technology Corporation (DTC) 029-9-92, Drexler Technology Corporation/Laser Card System Corporation, 1992 (Brochure)

[EYES94]   Eyestone, S. LTC, USAF, "Technical Coordination Meeting for the Multi-Technology Automated Reader Card (MARC), United States Air Force, 11 January 1994.

[FMS90]   Financial Management Service, *Applications of Computer Card Technology 1990*, Department of the Treasury, 1990.

[FLOO92]   Flood, S., "Smart Cards: U.S. Banks Take a "Wait and See" Approach to Tomorrow's ATMs," *Bank Marketing*, v. 24, n. 9, pp. 51-52, September 1992. DIALOG file 15, item 00639123.

[FONT93]   Fontanini, A., "Pay Phones: The Flexible Answer," *Telecommunications (International Edition)*, v. 27, n. 7, p. 65, July 1993. DIALOG file 15, item 00744337.

[GAO90]   GAO/IMTEC-90-88FS, "Space Data: Information on Data Storage Technologies," United States Government Accounting Office, pp. 1-19, September 1990.

[GATE90]   Gates, M., "Smart Cards: The Next Marketing Marvel?" *Incentive*, v. 164, n. 2, pp. 28-33, February 1990. DIALOG file 15, item 00487254.

[GEMPLUS]   Gemplus Card International, "Smart Card Standards," pp. 1-33.

[HADD93]   Haddock, R., "Building the Right Card Solution into Your Application," *CardTech/SecurTech 1993 Conference Proceedings*, CTST, Inc., pp. 381-390, 18 April 1993.

[HADE94]   Telephone conversation between D. Hadek, Toshiba American Electric Components, Incorporated, Product Marketing Engineering, Irvine, California and the author, 16 June 1994.

[HAEU93]   Haeuser, W., "Smart Card Manufacturing," *CardTech/SecurTech 1993 Conference Proceedings*, CTST, Inc., p. 33, April 1993.

[HEAD91]   Head, R., "Agency Interest in Smart Card Technology Grows," *Government Computer News*, v.10, n. 10, p. 87, 13 May 1991. DIALOG file 275, item 10771847.

[HERM91]   Herman, E. (Edith), "USDA Tests Smart Cards in Farmer-Support Pilots," *Federal Computer Week*, v. 5, n. 30, p. 6, 23 September 1991. DIALOG file 275, item 11699412.

[HOFI92]   Hoffman, T., "IS Leaders Working to Cure Societal Ills," *Computerworld*, v. 26, n. 32, p. 78, 10 August 1992. DIALOG file 15, item 00637789.

[HOFN92]   Hoffman, T., "NCR, AT&T Usher in "Smart" ATM Technology," *Computerworld*, v. 26, n. 50, p. 24, 14 December 1992. DIALOG file 15, item 00654169.

[HOLL93]   Holliday, K. K., "Debit Cards Win Starring Role," *Bank Marketing*, v. 25, n. 3, pp. 26-29, March 1993. DIALOG file 15, item 00699061.

[HOLO94]   "Holography," American Bank Note Holographics, Incorporated, 1994. (Brochure)

[HOWA82]   Howard, N., "Get Ready for the "Smart Card." *Dun's Business Month*, v. 119, n. 5, pp. 88-90, May 1982. DIALOG file 15, item 00171394.

[IACO91]   Iacobuzio, T., "U.S. to Test Food Stamp Smart Card," *Bank Systems & Technology*, v. 28, n. 1, p. 20, 22, January 1991. DIALOG file 15, item 00532295.

[INDU92]   "Industrial Engineering's 1992 Automatic Identification Buyer's Guide," *Industrial Engineering*, v. 24, n. 6, pp. BG1-BG16, June 1992. DIALOG file 15, item 00617680.

[INFO94]   "Information Spectrum, Inc.," Information Spectrum, Inc., 16 February 1994. (Brochure)

[INTERMEC]   Intermec, "Jet Poste Conference," American Production Services, Seattle. (Video Tape)

[ITKI92]   Itkin, S. and Martell, J., *A PDF 417 Primer*, Symbol Technologies, Inc., p. 15, April 1992.

[JOHN91]   Johnson, M., "Service Delivers Painless Insurance Claims," *Computerworld*, v. 25, n. 28, p. 27, 15 July 1991. DIALOG file 15, item 00561118.

[JOINT PUB 6-0] Department of Defense, Joint Pub 6-0, Office of the Chairman, The Joint Chiefs of Staff, Washington, D.C.

[KAEB92] Kaebnick, G. E., "Success for Optical Memory Cards After All?" *Inform*, v. 6, n. 4, p. 38-40, April 1992.

[KASS92] Kass, R., "Debit Redux," *Bank Systems & Technology*, v. 29, n. 12, pp. 46-50, December 1992. DIALOG file 15, item 00653991.

[KAWA94] Kawamoto, W., "Create-A-Check Brings New Meaning To Money Management," *Computer Shopper*, v. 14, n. 1, p. 530, January 1994. CD-ROM Computer Select Computer Library (TM).

[KAYE94] Kaye, M. P., "Clinical Application of Optical Cards," *CardTech/ SecurTech 1994 Conference Proceedings*, CTST, Inc., pp. 305-310, 10 April 1994.

[KIRS94] Kirschner, C. A., Maj., "Multi-technology Automated Reader Card (MARC) and Its Role in In-Transit Visibility (ITV)," *CardTech/ SecurTech 1994 Conference Proceedings*, CTST, Inc., p. 635, 10 April 1994.

[KROE92] Kroenke, D. M., *Database Processing*, Fourth Edition, McMillan Publishing Company, p. 79, 1992.

[KRUE94] Krueger, J., "Microcontrollers, ASICS, and Smart Cards," *CardTech/ SecurTech 1994 Conference Proceedings*, CTST, Inc., p. 51, 10 April 1994.

[KUTC92] Kutchera, A. W., "High Coercivity Media, What It Is And Why The Interest," *Card Tech Conference Proceedings*, p. 36, 7 April 1992.

[KUTF93] Kutler, J., "French Banks Try to Sell the U.S. on Smart Cards," *American Banker*, p. 16, 12 October 1993. CD-ROM Computer Select Computer Library (TM).

[KUTL93] Kutler, J., "Leader of Smart-Card Group Welcomes Some Competition," *American Banker*, p. 11, 27 October 1993. CD-ROM Computer Select Computer Library (TM).

[LAIR94] Interview between W. Laird, AMXLS-TE-A, PSCC ALOGS, Tobyhanna, PA and the author, 27 July 1994.

[LAT92] Los Angeles Times, "'Smart Card' Adds Brains to Credit Card," v. 111, p. 2, 26 May 1992. DIALOG file 275, item 12202868.

[LATA85]   Latamore, G. B., "Clever Cards," *Popular Computing*, v. 5, n. 1, pp. 35-36, November 1985. DIALOG file 275, item 00645626.

[LAUG93]   Laughlin, J., "Smart Cards in Tradeshows and Conventions," *CardTech/SecurTech 1993 Conference Proceedings*, CTST, Inc., p. 733, 18 April 1993.

[LAWL93]   Lawlor, M., "Microcircuit Technology Improves Readiness, Saves Resources," *SIGNAL, AFCEA's International Journal*, Reprint of SIGNAL Magazine, August 1993.

[LEFK94]   Lefkowitz, L., "PCMCIA Cards - Evolution or Just Confusion?" *PC Computing*, v. 7, n. 1, pp. 171 (11), January 1994. CD-ROM Computer Select Computer Library (TM).

[LEWI94]   Lewis, D., "Easy Money," *MacUser*, v. 10, n. 3, pp. 109(6), Ziff-Davis Publishing Company, March 1994. CD-ROM Computer Select COmputer Library (TM).

[LIND93]   Linden, L. F., "The World of Cards - An Overview," *CardTech/SecurTech 1993 Conference Proceedings*, CTST, Inc., pp. 3-18, 18 April 1993.

[LONG94]   Longwell, J., "PCMCIA Leads to the Future; Diverse New Technologies Lure Specialty Distributors," *Computer Reseller News*, n. 559, p. 101, 3 January 1994. CD-ROM Computer Select Computer Library (TM).

[LOUD94]   Loudermilk, S., "Modem Makers Slash Prices On PCMCIA Data/Fax Lines," *PC Week*, v. 11, n. 2, pp. 37 (2), Ziff-Davis Publishing Company, 17 January 1994. CD-ROM Computer Select Computer Library (TM).

[MADA92]   Madam, M. S. and Reid, M. A., "Data Processing Aspects of the Integrated Circuit and Magnetic Stripe Cards," *Information & Management*, v. 22, n. 1, pp. 41-52, January 1992.

[MALL93]   Mallory, J., "New for PC - Create a Check Corporate 4.1," *Newsbytes*, p. NEW12230024, 23 December 1993. CD-ROM Computer Select Computer Library (TM).

[MARC94]   "MARC Generic Architecture Requirements," Defense Information Service Agency (DISA), 1994.

[MART89]   Martres, D., "Le Smart Card," *Canadian Banker*, v. 96, n. 1, pp. 26-29, January/February 1989. DIALOG file 15, item 00438157.

[MCCR92]   McCrindell, J. Q., "Electronic Business Processes in Government,"
                CMA Magazine, v. 66, n. 10, p. 34, December 1992/January 1993.
                DIALOG file 15, item 00665339.

[MIL-L-61002]   Military Specification: Labels, Pressure-Sensitive Adhesive, for Bar
                Codes and other Markings, 15 June 1990.

[MIL-STD-499A] MIL-STD-499A   (USAF),   "Military   Standard   Engineering
                Management," Department of Defense, Washington, DC, 1 May 1974.

[MIL-STD-1189B] MIL-STD-1189B, "Military Standard: Standard Department of
                Defense Bar Code Symbology," Department of Defense, Washington,
                DC, 10 August 1989.

[MILB94]   Miller, B. F., "PCMCIA 2.1 Standards for Today and Tomorrow,"
                Windows Sources, v. 2, n. 1, p. 174, January 1994. CD-ROM Computer
                Select Computer Library (TM).

[MILL94]   Miller, B. F., "Biometric Identification: The Power to Protect People,
                Places   and   Privacy,"   *CardTech/SecurTech   1994   Conference
                Proceedings*, CTST, Inc., pp. 193-201, 10 April 1994.

[MILM84]   Mills, M., "Memory Cards: A New Concept in Personal Computing,"
                Byte, v. 9, n. 1, p. 154, January 1984. DIALOG file 275, item
                00527920.

[MILS93]   Miller, S. G., "Radio Frequency Identification Technology,"
                CardTech/SecurTech 1993 Conference Proceedings, CTST, Inc., pp.
                229-240, 19 April 1993.

[MITC92]   Mitchell, A. and Littlewood, S., "Marketing's Smart Transformation,"
                Marketing, pp. 16-18, 21 May 1992. DIALOG file 15, item 00622871.

[MITG93]   Mitchell, G. A., "Sub-Micron Technology and Smart Card Operating
                Environment (Systems)," *CardTech/SecurTech 1993 Conference
                Proceedings*, CTST, Inc., p. 60,71-76, 18 April 1993.

[MOOR92]   Moore, A. M., "Technology Explosion Shapes Marketing's Future,"
                Bank Marketing, v. 24, n. 5, pp. 24-27, May 1992. DIALOG file 15,
                item 00615749.

[MOOR94]   Moore, B., "Selecting a Bar Code Reader," *Automatic ID News*, p. 28,
                January 1994.

[MORA91]   Morant, A., "Payphones Evolve from Cash to Cards," *Telephone
                Engineer & Management*, v. 95, n. 7, pp. 55-57, 1 April 1991.
                DIALOG file 15, item 00543936.

[MOS92]   Mos, R. J., "High Coercivity Encoding," *Card Tech Conference Proceedings*, pp. 55-72, 7 April 1992.

[MUIR93]   Muir, B. A., "Authentication Considerations for External User Access," *CardTech/SecurTech 1993 Conference Proceedings*, CTST, Inc., pp. 899-903, 18 April 1993.

[MURP92]   Murphy, P. A., "Regional Networks Drive Debit Growth," *ABA Banking Journal*, v. 84, n. 9, pp. 68-76, September 1992.

[MURR94]   Murray, W. H., "Security Requirements of the Emerging Information Infrastructure," *CardTech/SecurTech 1994 Conference Proceedings*, CTST, Inc., pp. 963-970, 13 April 1994.

[NELS94]   Nelson, R. A., "Authentication Techniques for Smart Cards," *CardTech/SecurTech 1994 Conference Proceedings*, CTST, Inc., pp. 47-60, 13 April 1994.

[OMAL94]   O'Malley, C., "Hayes Card-Size Optima 144 is an Optimal Data/Fax Modem," *Computer Shopper*, v. 14, n. 2, p. 506, February 1994. CD-ROM Computer Select Computer Library (TM).

[OMDT93]   "Optical Memory: Drexler Technology Announces Highest Capacity Optical Memory Card - Data Storage Capacity Reaches 6.6 Megabyte - for Interactive Multimedia Applications", *Edge: Work-Group Computing Report*, v. 4, n. 167, p. 9, 2 August 1993. CD-ROM Computer Select Computer Library (TM).

[PALM91]   Palmer, R. C., *The Bar Code Book*, Second Edition, Helmers Publishing, Inc., 1991.

[PARK94]   Parker-Phillips, M., "Intermodal/Multi-Purpose Payments Model," *CardTechSecurTech 1994 Conference Proceedings*, CTST, Inc., pp. 639-648, 10 April 1994.

[PERR94]   Perry, W. J., "Specifications & Standards - A New Way of Doing Business," Secretary of Defense Memorandum, Washington, DC, 29 June 1994.

[PFLE89]   Pfleeger, C. P., *Security in Computing*, Prentice-Hall, Inc., 1989.

[PUNC92]   Punch, L., "ls Prepaid Debit Coming of Age?" *Credit Card Management*, v. 5, n. 7, pp. 10-14, October 1992. DIALOG file 15, item 00646584.

[REBO94]   Interview between M. Reboulet, Air Force AIT PMO, HQ AFMC/LGT (AIT), Wright-Patterson Air Force Base, OH and the author, 26 August 1994.

[RIST93]   Rist, O., "Power and Potential." *PC Magazine*, v. 12, n. 22, pp. 263 (10), 21 December 1993.

[ROTH93]   Rothfeder, J., "Holes in the Net," *Corporate Computing*, v.2, n. 5, pp. 114 (5), May 1993. CD-ROM Computer Select Computer Library (TM).

[RPAT94]   *Report of the Process Action Team of Military Specifications and Standards*, Office of the Under Secretary of Defense for Acquisition and Technology, Washington, DC, April 1994.

[RUSR91]   Russell, R. D., "Business Switched to Electronics for Access Control," *Security*, v. 28, n. 8, pp. 41-42, August 1991. DIALOG file 15, item 00570558.

[RUSS91]   Russell, D. and Gangemi, G.T. Sr., *Computer Security Basics*, O'Reilly & Associates, Inc., July 1991.

[SABE94]   Sabetti, A., "Radio Frequency Identification (RF/ID), Its Uses and Key Issues," *CardTech/SecurTech 1994 Conference Proceedings*, CTST, Inc., p. 396, 10 April 1994.

[SAMU92]   Samuel, M., "Non-Cash Alternatives and Money Laundering An American Model for Canadian Consumers' Protection," *American Business Law Journal*, v. 30, n. 2, pp. 169-222, September 1992. DIALOG file 15, item 00656757.

[SANT92]   Santosus, M., "What a Card!" *CIO*, v. 6, n. 5, pp. 64-67, December 1992. DIALOG file 15, item 00652525.

[SAVI94]   "Savi TyTag," Savi Technology, Mountain View, CA, 1994.

[SCHN91]   Schneider, K., "You Can't Keep A Smart Card Down," *Electronics Weekly*, n. 1551, p. 19, 1 May 1991. DIALOG file 275, item 10925010.

[SCST93]   "Smart Cards Speed Truck-Stop Transactions," *AT&T Technology*, v.8, n.1, p. 11, Spring 1993. DIALOG file 15, item 00711001.

[SEID93]   Seidman, S., "Advanced Card Technologies," *CardTech/SecurTech 1993 Conference Proceedings*, CTST, Inc., pp. 21-23, 18 April 1993.

[SEID94]   Seidman, S., "The State of Smart Card Technology," *CardTech/ SecurTech 1994 Conference Proceedings*, CTST, Inc., pp. 205-213, 11 April 1994.

[SFSC91]   "Standard for Smart Cards," *ComputerData*, v. 16, n. 4, p. 17, April 1991.DIALOG file 15, item 00548003.

[SHAF94]   Shaffer, R. A., "Don't Leave Home Without This," *Forbes*, v. 153, n. 1, p. 92, 3 January 1994. CD-ROM Computer Select Computer Library (TM).

[SHAR94]   Sharp, K. R., "Auto ID in the DoD," *ID Systems*, p. 40, July 1994.

[SHOM94]   Shomo, L. P., "Electronic Business Environment & Information Security," *CardTech/SecurTech 1994 Conference Proceedings*, CTST, Inc., pp. 999, 1013-1014, 13 April 1994.

[SIPP81]   Sippl, C. J., and Sippl, R. J., *Computer Dictionary*, 3rd. ed., Howard W. Sams & Co., Inc., 1981.

[SMIT87]   Smith, R. (Richard), "Enter The Smart Card," *Credit Management*, pp. 11-12, February 1987. DIALOG file 15, item 00350928.

[SOLT94]   Soltesz, J. A., "OMC -- Security and Identification, A New Approach," *CardTech/SecurTech 1994 Conference Proceedings*, CTST, Inc., p. 333, 10 April 1994

[SPAR94]   Sparks, R. L., "Optical Memory Card Application - Who is the Customer," *CardTech/SecurTech 1994 Conference Proceedings*, CTST, Inc., pp. 324-325, 10 April 1994.

[SPEC93]   Specht, Donald, W. J., "Optical Library Card Systems: A Non-Technical Perspective," *CardTech/SecurTech 1993 Conference Proceedings*, CTST, Inc., p. 215, 18 April 1993.

[STAM93]   Stam, N., "PCMCIA's System Architecture," *PC Magazine*, v. 12, n. 22, pp. 268-269, 21 December 1993. CD-ROM Computer Select Computer Library (TM).

[STEI87]   Steinberg, D., "On-line Claims Help Maryland Blue Cross Battle Competition," *PC Week*, v. 4, n. 22, pp. C1(2), 2 June 1987. DIALOG file 275, item 04960829.

[STEM93]   Stemp, R., "CS 4601 Computer Security Course Notes," Naval Postgraduate School, Monterey, CA, p. 10-35, January 1993.

[STON87]   Stone, P. S., "Bank Couples PCs, Micro Card to Increase Security: 'Smart' Cards Access Levels of Data Files," *InfoWorld*, v. 9, n. 31, p. 29, 3 August 1987. DIALOG file 275, item 05160352.

[SVIG87]   Svigals, J., *Smart Cards, The New Bank Card*, Macmillan Publishing Company, 1987.

[TABI93]   Tabibian, O. R., "Compact Connections," *PC Magazine*, v. 12, n. 22, pp. 275-290, 21 December 1993. CD-ROM Computer Select Computer Library (TM).

[TFLO91]   "The Future Look of Ship-to-Shore," *Communication News*, v. 28, n. 3, pp. 10-12, March 1991. DIALOG file 15, item 00555562.

[THOG83]   Thomas, G., "Smart Card Technology Catching on Slowly," *Credit*, v. 9, n. 6, pp. 22-23, November/December 1983. DIALOG file 15, item 00223158.

[THOM83]   Thompson, T. W., "The Smart Card - Tomorrow's Plastic," *United States Banker*, v. 94, n. 3, pp. 8-23, March 1983. DIALOG file 15, item 00200881.

[TMIS94]   "Theater Medical Information System (TMIS) Vision," Readiness & Deployable Division, Office of Medical Functional Integration Management, Deputy Under Secretary of Defense for Health Affairs, Briefing Notes, p. 9, 1994.

[TORE93]   Tores, C. and Walsh, T., "Out With The Old, In With Re-engineering," *American City & County*, v. 108, n. 6, pp. 49-50, May 1993. DIALOG file 15, item 00735418.

[TOWN93]   Townend, R. C., "Prepaid Cards ~ A Tour D'Horizon," *CardTech/ SecurTech 1993 Conference Proceedings*, p. 464, 18 April 1993.

[TOWT93]   Townend, R. C., "The Value of Collecting Plastic," *CardTech/ SecurTech 1993 Conference Proceedings*, p. 514, 18 April 1993.

[TUTT94]   Tuttle, J. R., "Open Protocols - The Keys to RF/ID Evolution," *CardTech/SecurTech 1994 Conference Proceedings*, CTST, Inc., pp. 361-386, 10 April 1994.

[VANC90]   Van Collie, S. C., "Top Technologies of the '90s," *Banking Software Review*, v. 15, n. 2, pp. 36-40, 1990. DIALOG file 15, item 00539672.

[VOSS94]   Vossel, R., "An Integrator's Perspective of RFID in Logistic Applications," *CardTech/SecurTech 1994 Conference Proceedings*, pp. 387-391, 10 April 1994.

[WEBB93]   Webb, D. PhD., "Kerberos: An Authentication Service for Open Network Systems," *CardTech/SecurTech 1993 Conference Proceedings*, CTST, Inc., pp. 853-867, 18 April 1993.

[WEBS88]   *Webster's II New Riverside University Dictionary*, The Riverside Publishing Company, 1988.

[WEND94]   Wendt, J. M., "Applying Hand Geometry to Time and Attendance," *CardTech/SecurTech 1994 Conference Proceedings*, CTST, Inc., pp. 419-423, 10 April 1994.

[WHAL82]   Whalen, B., "The 'Smart Card': No Longer a Solution in Search of a Problem," *Marketing News*, v. 16, n. 11, pp. 4-5, November 1982. DIALOG file 15, item 00188847.

[WHIT89]   Whitten, J. L., Bentley, L. D., and Barlow, V. M., *Systems Analysis & Design Methods*, Second Edition, Richard D. Irwin, Inc., p. 89, 1989.

[WIHO94]   "What is Holography?" American Bank Note Holographics, Incorporated, 1994.

[WNWD88]   *Webster's New World Dictionary of Computer Terms*, 3rd. ed., Webster's New World, 1988.

[WON91]   Won, D. J., "Introduction to Integrated Circuit (Smart) Cards," *Applied Systems Institute, Inc.*, pp. 1-13, 26 February 1991.

[ZAGU94]   Interview between J. Zagursky, AMXLS-TE-A, PSCC ALOGS, Tobyhanna, PA and the author, 27 July 1994.

[ZIFF94]   Ziff-Davis Publishing Company, "Can Notebooks Do Desktop Duty?" *PC Computing*, v. 7, n. 1, p. 173, January 1994. CD-ROM Computer Select Computer Library (TM).

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center   2
   Cameron Station
   Alexandria, VA 22304-6145

2. Dudley Knox Library   2
   Code 52
   Naval Postgraduate School
   Monterey, CA   93943-5002

3. Dr. Carl R. Jones   1
   Systems Management, Code AS/JS
   Naval Postgraduate School
   Monterey, CA   93943-5002

4. Roger Stemp   1
   Computer Science Department, Code CS/ST
   Naval Postgraduate School
   Monterey, CA   93943-5002

5. Lieutenant Leslie Bower   1
   R.D. #1, Box 487-B
   Beech Creek, PA 16822

6. Defense Logistic Studies Information Exchange   1
   U. S. Army Logistics Management College
   Fort Lee, VA 23801-6043

7. Commander   1
   Naval Computer and Telecommunication Command
   4401 Massachusetts Ave., N. W.
   Washington, DC 20394-5000

8. Defense Information Systems Agency   1
   TFEF
   3701 North Fairfax Drive
   Arlington, VA 22203-1713

9. Program Manager AIT (PM AIT)   1
   ATTN: SFAS-PS-TPC (MAJ Rasmussen)
   9350 Hall Road, Suite 142
   Fort Belvoir, VA 22060-5526

10. Air Force AIT Program Management Office (AIT PMO) 2
    HQ AFMC/LGT (AIT)
    MITLA Program Manager
    Attn: Mr. Mark Reboulet
    4375 Childlaw Road, Suite 6
    Wright-Patterson Air Force Base, OH 45433

11. Air Force AIT Program Management Office (AIT PMO 1
    HQ AFMC/LGT (AIT)
    MITLA Program Office
    Attn: Ms. Lisa Wagner
    4375 Childlaw Road, Suite 6
    Wright-Patterson Air Force Base, OH 45433

12. Office of the Assistant Secretary Of Defense (OASD) (C3I) 1
    ATTN: Michael Noll
    Information Technologies Resources
    Room 1C255, Pentagon
    Washington, DC 20301

13. Mr. Frank Murray 1
    Naval Supply Systems Command
    Code 4262B1
    Crystal Mall #3, Room 515
    1931 Jefferson Davis Highway
    Arlington, VA 22241-5360

14. LOGSA PSCC ALOGS 2
    ATTN: AMXLS-TE-A (Joe Zagursky)
    11 Midway Road
    Tobyhanna Army Depot
    Tobyhanna, PA   18466-5097

15. National Institute of Standards and Technology (NIST) 1
    Computer Security Division/Computer Systems Laboratory
    Gaithersburg, MD 20899

16. Federal Smart Card Users Group 1
    c/o Department of the Treasury
    Attn: Mr.John Moore
    Financial Management Service (FMS)
    Hyattsville, MD 20782

17. School of Industrial and Systems Engineering   1
    Attn: Dr. Chen Zhou
    765 Ferst Drive
    Atlanta, GA 30332

18. Information Spectrum, Inc.   1
    Attn: Mr. William Alsbrooks
    Vice President
    General Manager, National Headquarters
    One Skyline Tower
    5107 Leesburg Pike
    Falls Church, VA 22041

19. CANON U.S.A., Inc.   1
    Attn: Mr. Robert J. Callen
    Regional Manager, Optical Card Systems
    2051 Mission College Blvd.
    Santa Clara, CA   95054-1509

20. Intermec Corporation   1
    Attn: Mr. Roger C. Palmer, P. Eng.
    Vice President - Technology
    6001 36th Avenue West
    P. O. Box 4280 Mail Stop #760
    Everett, WA   98203-9280

21. Mr. Jeff Franklin   1
    Computer Security, Code 054
    Naval Postgraduate School
    Monterey, CA 93943-5002

22. Smart Card Forum   1
    Attn: Linnette Leatherwood
    3030 N. Rocky Point Dr. W.
    Suite 670
    Tampa, FL 33607

23. Smart Card Industry Association   1
    Executive Director
    Attn: Janet Sayer-Falls
    5600 General Washington Drive, Suite B-202
    Alexandria, VA 22312-2415

24. United States Military Academy (USMA)   2
    Directorate of Information Management (DOIM)
    ATTN: CPT Paul R. Logan
    West Point, NY 10996

25. Commander   1
    Naval Reserve Force
    COMNAVRESFOR (Code 104D)
    Attn: CDR William Demers
    4400 Dauphine Street
    New Orleans, LA 70148-5000

26. Commander   1
    Naval Air Reserve Force
    COMNAVAIRRESFOR (Code 504)
    Attn: LCDR J. Stewart
    4400 Dauphine Street
    New Orleans, LA 70148-5000

27. Commander Thomas Hoskins   1
    Computer Science Department, Code CS/H?
    Naval Postgraduate School
    Monterey, CA   93943-5002

27. Lieutenant Rudy G. Dollete   1
    1198 Sunbright Drive
    Oceanside, CA 92056